Cybercrime and the Law: Computer Fraud and Abuse Act (CFAA) and the 116th Congress

September 21, 2020

Congressional Research Service
https://crsreports.congress.gov
R46536

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R46536

September 21, 2020

Peter G. Berris
Legislative Attorney

Cybercrime and the Law: Computer Fraud and Abuse Act (CFAA) and the 116th Congress

The Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, is a civil and criminal cybercrime law prohibiting a variety of computer-related conduct. Although sometimes described as an anti-hacking law, the CFAA is much broader in scope. Indeed, it prohibits seven categories of conduct including, with certain exceptions and conditions:

1. Obtaining national security information through unauthorized computer access and sharing or retaining it;
2. Obtaining certain types of information through unauthorized computer access;
3. Trespassing in a government computer;
4. Engaging in computer-based frauds through unauthorized computer access;
5. Knowingly causing damage to certain computers by transmission of a program, information, code, or command;
6. Trafficking in passwords or other means of unauthorized access to a computer;
7. Making extortionate threats to harm a computer or based on information obtained through unauthorized access to a computer.

Since the original enactment of the CFAA in 1984, technology and the human relationship to it have continued to evolve. Although Congress has amended the CFAA on numerous occasions to respond to new conditions, the rapid pace of technological advancement continues to present novel legal issues under the statute. For example, with increasing computerization has come a corresponding proliferation of Terms of Service (ToS) agreements—contractual restrictions on computer use. But federal courts disagree on whether the CFAA imposes criminal liability for ToS violations, and the United States Supreme Court is currently considering a case on this issue. Another technological development that has created tension under the CFAA is the rise of botnets, which are networks of compromised computers often used by cybercriminals. Although the CFAA prohibits creating botnets and using them to commit certain crimes, it is unclear if selling or renting a botnet violates the statute—a potential concern given that botnet access is often rented from botnet brokers. On a more basic level, another change that has prompted some reexamination of the CFAA is the seemingly-growing frequency of computer crime. Some contend that the prevalence and perniciousness of hacking requires private actors to defend themselves by hacking back—that is, initiating some level of intrusion into the computer of the initial attacker. The same provisions of the CFAA that prohibit hacking ostensibly also make it a crime to hack back, which some legislation has sought to change.

Contents

Tables

Contacts

Introduction

Today, with computers more prevalent than ever before,[1] illicit computer-based activities such as hacking—intrusions or trespasses "into computer systems or data"[2]—are commonplace.[3] For example, on July 15, 2020, a malicious actor temporarily coopted the social media profiles of prominent politicians as part of an apparent scam to obtain cryptocurrency.[4] That same week, domestic and foreign intelligence agencies warned that hackers with an alleged connection to Russia are believed to be spying on coronavirus vaccine research in the United States and elsewhere.[5] Earlier in 2020, the Federal Bureau of Investigation (FBI) reported a spike in COVID-19-related phishing emails—messages designed to trick recipients into divulging personal information so the sender may access, for example, the recipient's email or bank accounts.[6]

Congress was prescient about the ubiquity of cybercrime nearly 40 years ago when it enacted the Computer Fraud and Abuse Act (CFAA)—a civil[7] and criminal law that prohibits a range of computer-based behaviors.[8] While a number of federal statutes may be relevant to combatting

[1] According to the United States Census Bureau (Census Bureau), by one measure only 8% of households had a computer in 1984. CAMILLE RYAN & JAMIE M. LEWIS, COMPUTER AND INTERNET USE IN THE UNITED STATES: 2015, U.S. CENSUS BUREAU 2 (Sept. 2017), https://www.census.gov/content/dam/Census/library/publications/2017/acs/acs-37.pdf. That same report indicated that the percentage increased to 87% of households in 2015, up from 84% in 2013. *Id.* For its part, the Federal Trade Commission has estimated that 50 billion devices will be connected to the Internet of Things (IoT) in 2020, a figure that includes internet-enabled devices such as smart appliances and fitness trackers. FEDERAL TRADE COMMISSION, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD i (Jan. 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf. For a review of Computer Fraud and Abuse Act (CFAA) issues unique to the IoT, see generally Sara Sun Beale & Peter Berris, *Hacking the Internet of Things: Vulnerabilities, Dangers, and Legal Responses*, 16 DUKE L. & TECH. REV. 161, 162 (Feb. 14, 2018). As discussed below, these devices are computers in the context of the CFAA. *See infra* § "Computer."

[2] United States v. Valle, 807 F.3d 508, 525 (2d Cir. 2015).

[3] In 2019, the Federal Bureau of Investigation's (FBI) Internet Crime Center (IC3) received 467,361 complaints regarding internet-enabled crimes—"an average of nearly 1,300 every day." FBI, *2019 Internet Crime Report Released* (Feb. 11, 2020), https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120. The actual number of computer and internet crimes is almost certainly higher, as many may escape detection entirely. *See* Beale, *supra* note 1, at 167–68 ("Additionally, in many cases consumers have little or no way to know when their . . . devices have been compromised . . . [as] [m]any objects connected to the internet continue to serve the function for which consumers purchased them long after their software becomes insecure."); *see also* Michel Cukier, *Study: Hackers Attack Every 39 Seconds*, A. JAMES CLARK SCH. OF ENG'G (Feb. 9, 2007), https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds#:~:text=A%20Clark%20School%20study%20is,attackers%20more%20chance%20of%20success (concluding that computers connected to the internet are attacked "every 39 seconds on average" by hackers).

[4] Philip Ewing, *Twitter Attack Underscores Broad Cyber Risks Still Facing U.S. Elections*, NPR (July 17, 2020), https://www.npr.org/2020/07/17/892044086/twitter-attack-underscores-broad-cyber-risks-still-facing-u-s-elections.

[5] Chris Fox & Leo Kelion, *Coronavirus: Russian Spies Target Covid-19 Vaccine Research*, BBC (July 16, 2020), https://www.bbc.com/news/technology-53429506.

[6] CRS Legal Sidebar LSB10446, *An Overview of Federal Criminal Laws Implicated by the COVID-19 Pandemic*, by Peter G. Berris.

[7] This Report cites to civil CFAA opinions as "most of the published cases interpreting § 1030 arise in the civil context rather than the criminal context" and "[c]ourts generally use civil and criminal interpretations of federal statutes interchangeably absent an indication that Congress intended a contrary approach." ORIN S. KERR, COMPUTER CRIME LAW 31, 75 (3d ed. 2013).

[8] H.R. REP. NO. 98-894, at 10 (1984) ("[B]y combining the ubiquity of the telephone with the capability of the personal computer, a whole new dimension of criminal activity becomes possible.").

nefarious computer activities such as those discussed above,[9] the CFAA is perhaps the most relevant, as it has been described as "the most important piece of U.S. legislation used to combat computer crime."[10]Among other things, the CFAA prohibits a person from trespassing into, damaging, or acquiring information from certain categories of computers, assuming the user lacks authorization for that conduct.[11] Indeed, prosecutors invoke the CFAA to combat a variety of computer-based activities.[12] Nevertheless, some have suggested that the rapid pace of technological change has rendered some provisions of the CFAA outmoded and difficult to apply to new technologies and emerging cybercrime threats.[13]

This report provides a brief overview of the CFAA and legal issues under the statute brought about by technological change—with primary emphasis on the CFAA's role as a criminal statute. The report begins with a history of the CFAA, before detailing the seven categories of conduct that the statute prohibits. After summarizing the remedies and penalties available for CFAA violations, the report provides a sketch of three select legal issues of possible interest for the 116th Congress. The first is whether the CFAA imposes criminal liability for violations of Terms of Service Agreements—contracts placing restrictions on computer use.[14] The Second involves the problem of individuals selling access to botnets, which are networks of infected computers often used by cybercriminals—transactions that may not be illegal under the CFAA.[15] Third, the Report describes the legal status of, and debate surrounding, hacking back—where the victim of a computer intrusion responds by hacking back against the original malicious actor.[16]

History of the CFAA

By many accounts, the history of the CFAA begins with a movie—the 1983 thriller *WarGames*[17] starring Matthew Broderick.[18] In *WarGames*, Broderick's character, a rebellious high school

[9] For example, relevant provisions might include, among others, federal laws criminalizing wire fraud under 18 U.S.C. § 1343, cyberstalking under 18 U.S.C. § 2261A, the interception of electronic communications under 18 U.S.C. § 2511, or the unlawful access of stored communications under 18 U.S.C. § 2701. For an examination of how these and other statutes apply to cybercrime, see generally U.S. DEP'T OF JUSTICE, COMPUTER CRIME & INTELLECTUAL PROPERTY SECTION, CRIMINAL DIVISION, PROSECUTING COMPUTER CRIMES (2015), https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf.

[10] DANIEL ETCOVICH & THYLA VAN DER MERWE, COMING IN FROM THE COLD: A SAFE HARBOR FROM THE CFAA AND THE DMCA § 1201 FOR SECURITY RESEARCHERS, BERKMAN KLEIN CTR. RSCH. PUBL'N NO. 2018-4, HARVARD UNIV. 7 (2018), https://dash.harvard.edu/bitstream/handle/1/37135306/ComingOutoftheCold_FINAL.pdf#page=11.

[11] 18 U.S.C. § 1030.

[12] *See* U.S. DEP'T OF JUSTICE, *supra* note 9, at 35 (providing examples of the types of conduct that may be prosecuted under just one of the CFAA's subsections).

[13] *See, e.g.*, Andrea M. Matwyshyn & Stephanie K. Pell, *Broken*, 32 HARV. J.L. & TECH. 479, 481 (2019) ("[O]ur definitive computer intrusion statute, the [CFAA], belies its last-century crafting, as it strains under the new threat vectors leveraged by this century's formidable attackers."); Amanda B. Gottlieb, *Reevaluating the Computer Fraud and Abuse Act: Amending the Statute to Explicitly Address the Cloud*, 86 FORDHAM L. REV. 767, 770 (2017) (expressing opinion that "in practice [the CFAA] has not been able to keep up with new innovations" and examining whether the law adequately protects computers connected to the cloud); Marcelo Triana, *Is Selling Malware A Federal Crime?*, 93 N.Y.U. L. REV. 1311, 1315 (2018) (examining whether the CFAA prohibits the sale of malware).

[14] *See generally* CRS Legal Sidebar LSB10423, *From Clickwrap to RAP Sheet: Criminal Liability under the Computer Fraud and Abuse Act for Terms of Service Violations*, by Peter G. Berris (examining judicial disagreement on the breadth of the CFAA with respect to Terms of Service Agreements violations).

[15] *See infra* § "Botnet Trafficking."

[16] *See infra* § "Hacking Back."

[17] WARGAMES (Metro-Goldwyn-Mayer Studios 1983).

[18] *See* Fred Kaplan, *'WarGames' and Cybersecurity's Debt to a Hollywood Hack*, N.Y. TIMES (Feb. 19, 2016),

student, nearly starts World War III when he accesses the computer system controlling the United States nuclear arsenal, mistaking the system for an interactive video game.[19] The movie's depiction of the dangers of the computer age—where even nuclear annihilation could be a few keystrokes away—was not lost on policy makers.[20] According to one report, after viewing WarGames at Camp David, President Ronald Reagan asked advisers and the chair of the Joint Chiefs of Staff whether the plot of the movie was possible.[21] The CFAA is sometimes "said to be the [eventual] result of their deliberations,"[22] although congressional interest in computer crimes may be traced back at least as far as the 1970s.[23]

The first major federal computer-crime enactment came in the form of the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 (the 1984 Act).[24] With exceptions, the law prohibited three subsets of computer-based conduct: (1) obtaining national security information through unauthorized computer access; (2) obtaining financial information through unauthorized computer access, and (3) trespassing into a government computer and "knowingly us[ing], modif[ying], destroy[ing], or disclos[ing] information" on that computer.[25] The 1984 Act faced a number of criticisms over its relatively narrow scope,[26] and the Department of Justice (DOJ) expressed concern that the 1984 Act made computer crime prosecutions difficult.[27] In 1986, Congress substantially amended the 1984 Act, and the modern CFAA has many of its roots in that 1986 amendment.[28] Among other things, the 1986 amendment modified intent requirements and prohibited new categories of conduct including password trafficking, damaging computers, and accessing computers with intent to defraud.[29] Since 1986, Congress has amended the CFAA on

https://www.nytimes.com/2016/02/21/movies/wargames-and-cybersecuritys-debt-to-a-hollywood-hack.html (describing the birth of federal cybersecurity laws following President Ronald Reagan's concern over the movie "WarGames"); Ivan Evtimov et al., *Is Tricking A Robot Hacking?*, 34 BERKELEY TECH. L.J. 891, 904 (2019) ("According to popular lore, President Reagan saw the movie *War Games* and met with his national security advisers the next day to discuss America's cyber vulnerabilities. The CFAA is said to be the result of their deliberations."); Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 429, 492 (2012) ("There is some evidence that when the CFAA was originally enacted in 1984, it was partially in response to the situations depicted in the action film WarGames.").

[19] *See* Roger Ebert, *WarGames*, ROGEREBERT.COM (June 3, 1983), https://www.rogerebert.com/reviews/wargames-1983 (reviewing and summarizing plot of *WarGames*).

[20] H.R. REP. NO. 98-894, at 10 (1984) (referencing *WarGames* in discussion of necessity of computer fraud legislation).

[21] Kaplan, *supra* note 18.

[22] Evtimov, *supra* note 18, at 904.

[23] *See* CRS Report 97-1025, *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws*, by Charles Doyle, at n.2 (chronicling legislative history of CFAA).

[24] Greg Pollaro, Note, *Disloyal Computer Use and the Computer Fraud and Abuse Act: Narrowing the Scope*, 2010 DUKE L. & TECH. REV. 12, 4 (Aug. 26, 2010).

[25] Pub. L. No. 98-473, § 2102, 98 Stat. 1837 (1984) (codified at 18 U.S.C. § 1030).

[26] *See, e.g.*, Jo-Ann M. Adams, *Controlling Cyberspace: Applying the Computer Fraud and Abuse Act to the Internet*, 12 SANTA CLARA COMPUTER & HIGH TECH. L.J. 403, 422 (1996) ("[The 1984 Act] protected a very narrow class of financial and credit information.").

[27] *See generally* S. REP. NO. 99-432, at 6–9 (1986) (summarizing concerns expressed by DOJ).

[28] Adams, *supra* note 26, at 422.

[29] *Id.* at 423.

numerous occasions,[30] broadening both the conduct prohibited by the statute and the types of computers protected.[31] Today, the CFAA is the main federal[32] computer fraud statute.[33]

Overview of the CFAA

Key CFAA Terms

Although the CFAA is the primary federal anti-hacking statute,[34] the word "hacking" does not appear in any of its various provisions.[35] Instead, the statute criminalizes several categories of conduct that include many types of computer hacking as well as a variety of other computer-based activities.[36] Each category of conduct that the CFAA criminalizes tends to be defined by several overarching key terms that appear throughout the CFAA. Generally, the CFAA prohibits conduct that (1) is carried out by an individual "without authorization" or who "exceeds authorized access," and that (2) involves a computer.[37] Thus, the meanings of "computer," "without authorization," and "exceeds authorized access" are all crucial to understanding the scope of the CFAA.

Computer

The CFAA broadly[38] defines "computer" as any "electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions," including "any data storage facility or communications facility directly related to or operating in conjunction with such device . . . ."[39] The CFAA excludes only automated typewriters, typesetters, portable hand held calculators, and similar devices from its definition of computer.[40] These limited exceptions to the CFAA's definition of "computer" "show just how general" the statute's definition of computer is.[41] As one court explained, the definition includes any device with an electronic data processor, of which there are numerous examples.[42] Thus, under the CFAA, computers include not only laptops and desktops, but also a wide array of computerized

[30] *See* Doyle, *supra* note 23, at n.2 (listing CFAA amendments).

[31] *See* U.S. DEP'T OF JUSTICE, *supra* note 9, at 1–2 (summarizing amendments to CFAA).

[32] The CFAA exists against the backdrop of numerous state computer crime laws that are beyond the scope of this Report. *E.g.,* VT. STAT. ANN. tit. 13, §§ 4101–07. Computer misuse statutes have been enacted in "all fifty states . . . ." KERR, *supra* note 7, at 29; *accord Computer Crime Statutes,* NAT'L CONF. OF STATE LEGISLATURES (Feb. 24, 2020), https://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx (conducting survey of the computer crime laws of all 50 states).

[33] *See* Evtimov, *supra* note 18, at 904 ("Since its implementation, the CFAA has been the nation's predominant anti-hacking law.").

[34] *See id.*

[35] *See* 18 U.S.C. § 1030 (proscribing various conduct without use of the word "hacking").

[36] *Id.*

[37] *See, e.g., id.* § 1030(a)(2) (prohibiting "intentionally access[ing] a computer without authorization" or in excess of authorization, and obtaining certain types of information).

[38] *See* United States v. Mitra, 405 F.3d 492, 495 (7th Cir. 2005) (discussing breadth of CFAA with respect to the types of computers it governs).

[39] 18 U.S.C. § 1030(e)(1).

[40] *Id.*

[41] *Mitra*, 405 F.3d at 495 (emphasis omitted).

[42] United States v. Kramer, 631 F.3d 900, 902 (8th Cir. 2011).

devices ranging from cellphones to objects embedded with microchips, such as certain microwave ovens, watches, and televisions.[43]

Protected Computers

Several provisions within the CFAA specifically concern "protected computers."[44] Among other things, the CFAA defines protected computers as those that are either "exclusively for the use of a financial institution or the United States Government" or that are "used in or affecting interstate or foreign commerce or communication . . . ."[45] Courts have construed the latter phrase as including any computer connected to the internet.[46] Thus, most modern computing devices are subject to the CFAA's protections, including Internet of Things devices such as smart appliances and fitness trackers.[47] Another important type of computer that fits within the definition of protected computer is a server—a computer that manage website data and other information.[48] For example, courts have concluded that the web servers storing and sharing the member data of a large social media website qualified as protected computers.[49]

[43] *Id.* at 902–03; *accord* United States v. Nosal, 844 F.3d 1024, 1050 (9th Cir. 2016) ("This means that nearly all desktops, laptops, servers, smart-phones, as well as any 'iPad, Kindle, Nook, X–box, Blu–Ray player or any other Internet-enabled device,' including even some thermostats qualify as [protected computers]." (quoting United States v. Nosal, 676 F.3d 854, 861 (9th Cir. 2012)); Berris, *supra* note **Error! Bookmark not defined.**, at 2 (describing CFAA as "an anti-hacking law covering most computers, including laptops, desktops, websites, and computerized devices").

[44] 18 U.S.C. § 1030.

[45] *Id.* § 1030(e)(2).

[46] *See, e.g.*, hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985, 999 (9th Cir. 2019) ("The term 'protected computer' refers to any computer 'used in or affecting interstate or foreign commerce or communication,' . . . effectively any computer connected to the Internet . . . including servers, computers that manage network resources and provide data to other computers." (quoting 18 U.S.C. § 1030(e)(2)(B)) (internal citations omitted)).

[47] Although federal cases specifically examining the CFAA's applicability in the context of the Internet of Things are scarce, the general consensus among observers is that internet-enabled objects qualify as protected computers. *E.g.*, Beale, *supra* note 1, at 170; *accord* Matthew Ashton, Note, *Debugging the Real World: Robust Criminal Prosecution in the Internet of Things*, 59 ARIZ. L. REV. 805, 813 (2017) ("Phones, tablets, Fitbits, and even public transit cards with embedded computer chips are all included in the definition of a *protected computer*."); TJ Wong, *Is My Toaster a Computer? The Computer Fraud and Abuse Act's Definition of "Protected Computer" in the Age of the Internet of Things*, COLUMB. J.L. & SOC. PROBS. (Mar. 30, 2019), http://jlsp.law.columbia.edu/2019/03/30/is-my-toaster-a-computer-the-computer-fraud-and-abuse-acts-definition-of-protected-computer-in-the-age-of-the-internet-of-things/ (explaining that the definition of computer includes "all IOT devices feeding us data online, such as fitness watches and voice assistants," which means that in "the age of IOT, the CFAA's definition of 'protected computers' expands to cover items beyond the plain meaning of the term" including toasters and refrigerators).

One interesting example from case law is that of *United States v. Peterson*. 776 F. App'x 533 (9th Cir. 2019). In *Peterson*, the Federal Court of Appeals for the Ninth Circuit considered a vagueness challenge to a condition of supervised release imposed on a defendant convicted of possessing child pornography. *Id.* at 533. The condition at issue restricted the defendant from accessing a computer as defined by the CFAA. *Id.* at 534. In agreeing with the defendant that the condition was potentially overbroad, the court observed that a wide range of objects fall within the definition of computer under the CFAA, including "refrigerators with Internet connectivity, Fitbit™ watches" and certain automobiles. *Id.* at n.3. Although the court did not discuss these devices in relation to the phrase "protected computer," it described them in a manner that would satisfy the definition of protected computer under the CFAA; as the court noted, Internet of Things devices are (1) computers (2) connected to the internet. *Id.*

[48] *hiQ Labs, Inc.*, 938 F.3d at 999.

[49] *Id.*

Without Authorization and Exceeds Authorized Access

Numerous provisions in the CFAA only apply if the defendant acts "without authorization" or if he "exceeds authorized access" when committing the relevant conduct.[50] For example, Section 1030(a)(2) prohibits intentionally accessing a computer without authorization or in excess of authorization and obtaining information from a financial institution, the federal government, or a protected computer.[51] Other provisions contain nearly identical requirements.[52]

While the CFAA repeatedly uses the phrases "exceeds authorized access" and "without authorization," the statute does not fully define either phrase.[53] In fact, the statute offers no definition for "without authorization."[54] And, although the CFAA does explain that "exceeds authorized access" means "access[ing] a computer *with authorization* and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter," that definition hinges on the meaning of the undefined phrase "with authorization."[55]

On a more fundamental level, the meaning of authority—the common concept in "exceeds authorized access" and "without authorization"—is also undefined by the CFAA.[56] In practice, it appears that authority to use a computer may be positively granted in a number of ways—for example through an employer who lets an employee use a work computer for business purposes[57] or a website that allows users to access its servers for some function.[58] But the scope of authority—and therefore its meaning under the CFAA—largely depends on the negative limits placed on that authority in the specific context in which the statute is applied.[59] As a result, it is difficult if not impossible to separate authority from the phrases "exceeds authorized access" and "without authorization," as those phrases represent the outer boundaries of authorized computer use.[60] And those boundaries are hazy under the CFAA; courts, for example, disagree on the extent to which authority may be curtailed by contractual restrictions,[61] as opposed to technological restrictions such as password requirements.[62]

---

[50] 18 U.S.C. § 1030.

[51] *Id.* § 1030(a)(2).

[52] *Id.* § 1030.

[53] *Id.*

[54] *Id.* § 1030(e).

[55] *Id.* (emphasis added).

[56] *Id.* § 1030.

[57] *See, e.g.*, United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010) (explaining that employee was authorized by employer to use database).

[58] hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985, 1002 (9th Cir. 2019) (examining authority to access information on website servers as byproduct of that information being generally available to the public).

[59] *See, e.g.*, *Rodriguez*, 628 F.3d at 1263 (describing scope of employee's authority to use databases by its outer limit, specifically that "use of databases to obtain personal information is authorized only when done for business reasons"); Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1067 (9th Cir. 2016) (describing how authorization was removed by a written cease and desist letter).

[60] *See, e.g., hiQ Labs, Inc.*, 938 F.3d at 1003 (exploring limits of authority based on whether use of a computer fell into the "without authorization" category as a result of a cease and desist letter).

[61] Indeed, there is an unresolved split in the federal courts of appeals over whether "without authorization" and "exceeds authorized access" permit criminal liability for violations of contracts restricting the permissible uses of a given computer, such as employer computer use policies or ToS agreements—contracts that govern the use of a product such as a website. *See infra* § "The CFAA and ToS Violations."

[62] *See infra* § "The CFAA and ToS Violations." One scholar has suggested three types of restrictions that may limit authorized computer use, including: (1) code based restrictions such as passwords or other means of programming

Even if the meanings of "exceeds authorized access" and "without authorization" are unclear, there is some indication in legislative history that the two phrases were intended to correspond to different categories of unauthorized computer use.[63] At least in theory, the intent was for "without authorization" to apply to outsiders such as hackers,[64] who are "wholly lacking in authority to access or use [the relevant] computer."[65] In contrast, it appears that "exceeds authorized access" may have been meant to apply to insiders[66] such as employees who have some authorization to use a computer, but who surpass that authority.[67] For example, the Senate Report accompanying the 1986 amendment to the CFAA reflects a concern that § 1030(a)(3)—which prohibits trespassing in government computers—would be interpreted "so broad[ly] as to create a risk that government employees and others who are authorized to use a Federal Government computer would face prosecution" when they went beyond their authorization.[68] According to that report, to prevent the application of the law to such insiders, the "Committee [on the Judiciary] declined to criminalize acts in which the offending employee merely 'exceeds authorized access . . . .'"[69]

Whatever the legislative intent, judicial interpretations of "without authorization" and "exceeds authorized access" have not been entirely consistent, and as one court opined, the difference between the terms is "paper thin."[70] Some courts have maintained the distinction between insiders and outsiders with respect to "exceeds authorized access" and "without authorization:" concluding that insiders may act without authorization only after their authorization has been terminated by an affirmative act such as a cease and desist letter.[71] Similarly, some courts have concluded that "without authorization" applies only to individuals who have no right to access a computer whatsoever, such as those who bypass password requirements[72] or who otherwise "circumvent[] technological access restrictions."[73] But broader interpretations of "without authorization" have been applied in other jurisdictions, including by some courts that have held that insiders may act without authorization if they breach a duty of loyalty to an employer.[74]

---

hardware or software to restrict access; (2) contractual restrictions such as Terms of Service agreements; and (3) social norms of computer use. KERR, *supra* note 7, at 40–41.

[63] *See* U.S. DEP'T OF JUSTICE, *supra* note 9, at 5–6 (recounting legislative history regarding intended meanings of "exceeds authorized access" and "without authorization").

[64] S. REP. No. 104-357, at 9 (1996) (describing outsiders as those "who gain access to a computer without authorization.").

[65] S. REP. No. 99-432, at 8 (1986).

[66] *See* S. REP. No. 104-357, at 6 (1996) ("The amendment specifically covers the conduct of . . . an insider who exceeds authorized access . . . .").

[67] S. REP. No. 99-432, at 8 (1986) (describing "purely 'insider' cases" as those of individuals "who, while authorized to use some computers in their department, use others for which they lack the proper authorization.").

[68] *Id.* at 7.

[69] *Id.*

[70] Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006). According to Professor Orin S. Kerr, "technological changes have blurred the line between" the phrases "without authorization" and "exceeds authorized access." Brief of Professor Orin S. Kerr as Amicus Curiae in Support of Petitioner, Van Buren v. United States, No. 19-783, 2020 WL 4003433, at *16 (U.S. July 8, 2020).

[71] *See, e.g.*, LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1135 (9th Cir. 2009) ("Rather, we hold that a person uses a computer 'without authorization' under §§ 1030(a)(2) and (4) when the person has not received permission to use the computer for any purpose (such as when a hacker accesses someone's computer without any permission), or when the employer has rescinded permission to access the computer and the defendant uses the computer anyway.").

[72] *See, e.g.*, Pulte Homes, Inc. v. Laborers' Int'l Union of N. Am., 648 F.3d 295, 304 (6th Cir. 2011) (holding that party did not act without authorization by accessing an "unprotected public communications system[]").

[73] Brief of Professor Orin S. Kerr as Amicus Curiae in Support of Petitioner, *supra* note 70, at *16.

[74] *See Int'l Airport Ctrs., LLC*, 440 F.3d at 420 (holding that employee's authorization to use employer's computer

Prohibited Conduct Under the CFAA

The CFAA prohibits seven categories of conduct, ranging from certain acts of computer trespass to unauthorized computer access with an intent to defraud.[75]

Cyber Espionage, 18 U.S.C. § 1030(a)(1)

Section 1030(a)(1)[76] is a cyber-espionage provision that in certain instances prohibits obtaining and sharing national security information[77]—such as "information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations . . . ."[78] According to the DOJ, examples of national security information under § 1030(a)(1) could include "classified information obtained from a Department of Defense computer or restricted data obtained from a Department of Energy computer."[79] Nevertheless, in practice, the provision has been rarely invoked, if at all,[80] perhaps because prosecutors charge offenses involving national security information under federal espionage statutes that overlap with § 1030(a)(1).[81]

Prosecutions under § 1030(a)(1) require the government to establish several elements beyond a reasonable doubt. First, the government would need to prove that the defendant obtained the national security information by knowingly[82] accessing a computer without authorization or in

terminated where he breached duty of loyalty and improperly erased employer's data).

[75] The content of this section draws heavily from Doyle, *supra* note 23.

[76] 18 U.S.C. § 1030(a)(1) imposes criminal penalties on:

> (a) Whoever--
>
> > (1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it.

[77] Doyle, *supra* note 23, at 71–72 (noting that § 1030(a)(1) "essentially tracks existing federal espionage laws" and prohibits the willful disclosure, attempted disclosure, or failure to return "classified information concerning national defense, foreign relations, or atomic energy" when certain conditions are met).

[78] 18 U.S.C. § 1030(a)(1).

[79] U.S. DEP'T OF JUSTICE, *supra* note 9, at 13.

[80] *See* KERR, *supra* note 7, at 30 ("Although it is the first in the list of § 1030(a) crimes, [§ 1030(a)(1)] appears never to have been used.").

[81] *See, e.g.*, Press Release, U.S. Dep't of Justice, Defense Department Linguist Charged with Espionage (Mar. 4, 2020), https://www.justice.gov/opa/pr/defense-department-linguist-charged-espionage (announcing charges against defendant under espionage statutes rather than § 1030(a)(1) for alleged conduct including improperly accessing United States Department of Defense "classified systems" which defendant "had no need to access" and transmitting that information to "a foreign terrorist organization"); *accord* U.S. DEP'T OF JUSTICE, *supra* note 9, at 15 ("In situations where both [§ 1030(a)(1) and a federal espionage statute] . . . are applicable, prosecutors may tend towards using [the espionage statutes], for which guidance and precedent are more prevalent.").

[82] Although the CFAA does not define "knowingly," and despite a dearth of case law on § 1030(a)(1), a Senate Report accompanying the 1986 amendment to the CFAA noted that a knowing act is one where the person is aware "that the result is practically certain to follow from his conduct, whatever his desire may be as to that result." S. REP. NO. 99-432,

excess of authorization.[83] Notably, § 1030(a)(1) broadly covers all computers, as opposed to just protected computers.[84] Second, a § 1030(a)(1) violation requires the government to establish that the defendant had reason to believe that the information could cause "injury to the United States" or benefit "any foreign nation."[85] There is little case law expounding on this element, but the DOJ has indicated that it can likely be satisfied where "the national security information is classified or restricted" and the defendant was aware of that fact.[86] Finally, the government must prove that the defendant "willfully communicate[d], deliver[ed], transmit[ted] or . . . retain[ed]" the national security information, or attempted to do so, or caused the communication, delivery, or transmission of national security information.[87] This element is broad, and by its own terms includes a range of activities including the failure to return national security information or the disclosure of that information.[88] However, such behavior must be intentional.[89]

Obtaining Information by Unauthorized Computer Access, 18 U.S.C. § 1030(a)(2)

Section 1030(a)(2)[90] generally prohibits accessing a computer without authorization or in excess of authorization and obtaining information in certain circumstances. Although at first glance it could appear that to "obtain information" might refer specifically to misappropriation or theft of information, the concept is much broader.[91] Indeed, as interpreted by courts, "obtaining information" includes "mere observation of the data" such as looking at or reading information on a screen.[92] Perhaps unsurprisingly then, the government has invoked § 1030(a)(2) in a variety of

---

at 6 (1986) (quoting United States v. U.S. Gypsum Co., 438 U.S. 422, 445 (1978)). That description tracks judicial interpretations of the word knowing under other subsections of the CFAA, where courts have concluded that the term excludes accidental behavior. *See* QVC, Inc. v. Resultly, LLC, 99 F. Supp. 3d 525, 536 (E.D. Pa. 2015) (concluding that § 1030(a)(5)(A) requires showing that "defendant intended to cause harm" and that "[d]amage caused by mere recklessness or negligence is insufficient").

[83] 18 U.S.C. § 1030(a)(1).

[84] *Id.*

[85] *Id.*

[86] U.S. DEP'T OF JUSTICE, *supra* note 9, at 14.

[87] 18 U.S.C. § 1030(a)(1).

[88] *Id.*

[89] *Id.*

[90] Section 1030(a)(2) imposes criminal liability on:

> (a) Whoever--
>
> > (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains--
> >
> > > (A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);
> >
> > > (B) information from any department or agency of the United States; or
> >
> > > (C) information from any protected computer.

[91] *See* United States v. Drew, 259 F.R.D. 449, 457 (C.D. Cal. 2009) ("'Obtain[ing] information from a computer' has been described as 'includ[ing] mere observation of the data. Actual aspiration . . . need not be proved in order to establish a violation . . . .'" (alterations in original) (quoting S. REP. NO. 99-432, at 6–7 (1986))); Am. Online, Inc. v. Nat'l Health Care Disc., Inc., 121 F. Supp. 2d 1255, 1276 (N.D. Iowa 2000) (looking to legislative history for the preposition that § 1030(a)(2) covers not just theft but also the observation of data).

[92] *See Drew*, 259 F.R.D. at 457 n.13 ("[T]he term 'obtaining information' includes merely reading it." (alteration in

prosecutions,[93] including that of a former police sergeant for using a restricted law enforcement database for non-law enforcement purposes[94] and an Italian citizen for "hack[ing] into thousands of computers without permission [and] . . . gaining access to all of the information stored on those computers."[95]

Although they do not significantly limit the provision's scope, there are three additional statutory requirements that the government must satisfy to prove a § 1030(a)(2) violation.[96] First, § 1030(a)(2) requires *intentional* access to a computer by the defendant, "rather than mistaken, inadvertent, or careless" access.[97] However, the intent requirement is a low bar to prosecution because intent to obtain information is not required; instead all that is required is intent to access a computer without authorization or in excess of authorization.[98] Second, the defendant's access must be without authorization or in excess of authorization—elements that are discussed above. Finally, for § 1030(a)(2) to apply, the information must be obtained from either a financial institution,[99] the federal government, or "any protected computer."[100] As discussed, any computer connected to the internet suffices. Thus, as one court explained, barring a narrow interpretation of "without authorization" or "exceeds authorized access," it is possible that § 1030(a)(2) could criminalize any conscious violation of ToS or other contractual restrictions on computer use.[101] As discussed below, however, prosecutorial discretion and DOJ charging policies may in practice restrict the application of provisions such as § 1030(a)(2) to some degree.

Government Computer Trespassing, 18 U.S.C. § 1030(a)(3)

Section 1030(a)(3)[102] generally prohibits intentionally accessing a government computer without authorization. It is "a simple trespass offense,"[103] which at common law often refers to an unsanctioned entry on to the land of another, regardless of whether that entry caused any harm.[104]

---

original) (quoting S. REP. NO. 104–357, at 7 (1996))).

[93] Section 1030(a)(2) is "the most commonly charged section of the [CFAA]." KERR, *supra* note 7, at 76.

[94] United States v. Van Buren, 940 F.3d 1192, 1198 (11th Cir. 2019), *cert. granted*, No. 19-783, 2020 WL 1906566 (U.S. Apr. 20, 2020).

[95] United States v. Gasperini, 894 F.3d 482, 487 (2d Cir. 2018).

[96] *See generally* KERR, *supra* note 7, at 78–79 (explaining breadth of § 1030(a)(2) and why requirements in that provision pose "relatively low thresholds").

[97] S. REP. NO. 99-432, at 5 (1986).

[98] *Drew*, 259 F.R.D. at 467 ("The only scienter element in section 1030(a)(2)(C) is the requirement that the person must 'intentionally' access a computer without authorization or 'intentionally' exceed authorized access.").

[99] The provision also includes information obtained from card issuers and consumer reporting agencies. 18 U.S.C. § 1030(a)(2).

[100] 18 U.S.C. § 1030(a)(2).

[101] *Drew*, 259 F.R.D. at 457.

[102] 18 U.S.C. § 1030(a)(3) imposes criminal liability on:

> (a) Whoever--
>
> > (3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States.

[103] S. REP. NO. 99-432, at 7 (1986) (clarifying that § 1030(a)(3) "applies to acts of simple trespass against computers belonging to, or being used by or for, the Federal Government").

[104] *E.g.*, Restatement (Second) of Torts § 158 (1965). Criminal liability for trespass—under various statutes—often involves additional requirements such as notice to a person that he is trespassing, followed by that person's knowing

Thus, unlike the previous two CFAA prohibitions, the crux of a § 1030(a)(3) violation is unauthorized entry into government computers, and the provision does not require that the defendant do anything with, or obtain anything from, the covered computer once he has accessed it.[105] The provision is seldom invoked by prosecutors, likely because it overlaps significantly with § 1030(a)(2), which imposes stricter penalties.[106]

There are two ways the government can establish a § 1030(a)(3) violation.[107] First, the government may demonstrate that the defendant accessed a "nonpublic computer of a department or agency of the United States" used *exclusively* by the federal government.[108] A nonpublic computer includes one for internal use, such as the data servers of a federal agency.[109] The term nonpublic computer excludes, however, public-facing government computers, internet servers, and websites, such as those offering public services or information.[110] Second, the government may establish a § 1030(a)(3) violation where the defendant accesses a "nonpublic computer of a department or agency of the United States," if that computer is used *in part* by the federal government and the defendant's "conduct affects that use."[111] A computer used in part by the federal government might include, for example, a private company's computer on which the federal government has an account.[112] In practice, "[a]lmost any network intrusion will affect the government's use of its computers because any intrusion potentially affects the confidentiality and integrity of the government's network and often requires substantial measures to assure the integrity of data and the security of the network."[113]

Regardless of the nature of the § 1030(a)(3) violation, the government must prove that the defendant's access was intentional and without authorization.[114] The intent requirement is identical to the one in § 1030(a)(2). Although the meaning of "without authorization" is also discussed above,[115] it is notable that the statute excludes liability where the defendant's conduct merely exceeds authorized access.[116] Based on legislative history, it appears that such language was omitted to foreclose criminal liability against those who have some authorization, like federal employees approved to use a government computer, but who do so in an unapproved manner.[117]

---

refusal to vacate the area in which he is trespassing. *E.g.*, CONN. GEN. STAT. § 53a-107.

[105] Doyle, *supra* note 23, at 3 (explaining that "nothing more than unauthorized entry is required" to violate § 1030(a)(3).

[106] *See* U.S. DEP'T OF JUSTICE, *supra* note 9, at 23, 25 (explaining why § 1030(a)(2) may be the "preferred charge" in instances where both § 1030(a)(2) and § 1030(a)(3) could apply).

[107] 18 U.S.C. § 1030(a)(3).

[108] *Id.*

[109] *See* U.S. DEP'T OF JUSTICE, *supra* note 9, at 24 ("'Nonpublic' includes most government computers, but not Internet servers that, by design, offer services to members of the general public.").

[110] *Id.*

[111] 18 U.S.C. § 1030(a)(3).

[112] U.S. DEP'T OF JUSTICE, *supra* note 9, at 24.

[113] *Id.*; *accord* Sawyer v. Dep't of Air Force, 31 M.S.P.R. 193, 196 (1986) ("The elements for establishing a criminal violation of 18 U.S.C. § 1030(a)(3) . . . do not include the requirement that the prohibited access to the computer system be for the specific purpose of defrauding the government. Rather, that statutory provision defines as a criminal violation the knowing unauthorized access or use of the system for any unauthorized purpose.").

[114] 18 U.S.C. § 1030(a)(3).

[115] *See supra* § "Without Authorization and Exceeds Authorized Access."

[116] *Id.*

[117] As noted in S. REP. NO. 99-432, at 7 (1986):

> The Committee wishes to be very precise about who may be prosecuted under the new subsection

Computer Fraud: 18 U.S.C. § 1030(a)(4)

Section 1030(a)(4)[118] is an anti-fraud provision, which makes it a crime to "knowingly and with intent to defraud, access[] a protected computer without authorization, or exceed[] authorized access" and obtain anything of value, or use of the computer itself if that use is worth at least $5,000 a year.[119] Prosecutors have used § 1030(a)(4) to charge a variety of fraudulent activity involving computers, including the use of a lottery terminal to falsely generate winning tickets,[120] a phishing scheme that netted "hundreds of thousands of dollars,"[121] and a plot to use misappropriated computer credentials to inflate grades at two universities.[122]

To prove a violation of § 1030(a)(4), the government must first establish that the defendant "knowingly and with intent to defraud, access[ed] a protected computer without authorization, or exceed[ed] authorized access." The statute does not define what it means to act knowingly and with intent to defraud in the context of § 1030(a)(4).[123] However, in the context of a civil § 1030(a)(4) claim, at least one federal court has explained that "intent to defraud" means to act "willfully and with specific intent to deceive or cheat, usually for the purpose of getting financial gain for one's self or causing financial loss to another."[124] Further guidance on the meaning of "knowingly and with intent to defraud" may be found in the legislative history of § 1030(a)(4), which notes that the identical standard is also employed in 18 U.S.C. § 1029, which governs credit card fraud.[125] In the context of § 1029, "knowingly and with intent to defraud" means "that the offender is conscious of the natural consequences of his action (i.e., that it is likely that

---

> (a)(3). The Committee was concerned that a Federal computer crime statute not be so broad as to create a risk that government employees and others who are authorized to use a Federal Government computer would face prosecution for acts of computer access and use that, while technically wrong, should not rise to the level of criminal conduct. At the same time, the Committee was required to balance its concern for Federal employees and other authorized users against the legitimate need to protect Government computers against abuse by "outsiders."

[118] 18 U.S.C. § 1030(a)(4) imposes criminal liability on whoever:

> [K]nowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period.

[119] *Id.*

[120] United States v. Bae, 250 F.3d 774, 775 (D.C. Cir. 2001).

[121] United States v. Iyamu, 356 F. Supp. 3d 810, 814 (D. Minn. 2018).

[122] United States v. Barrington, 648 F.3d 1178, 1184 (11th Cir. 2011).

[123] U.S. DEP'T OF JUSTICE, *supra* note 9, at 27 ("The phrase 'knowingly and with intent to defraud' is not defined by section 1030. Very little case law under section 1030 exists as to its meaning, leaving open the question of how broadly a court will interpret the phrase.").

[124] Fidlar Techs. v. LPS Real Estate Data Sols., Inc., 82 F. Supp. 3d 844, 851 (C.D. Ill. 2015) (quoting United States v. Henningsen, 387 F.3d 585, 590–91 (7th Cir. 2004)), *aff'd*, 810 F.3d 1075 (7th Cir. 2016); *see also* United States v. Nosal, 676 F.3d 854, 864 (9th Cir. 2012) (Silverman J., dissenting) (concluding that § 1030(a)(4) requires specific intent to defraud). More generally, other federal courts that have concluded that to "defraud" under § 1030(a)(4) refers broadly to wrongdoing rather than to the specific elements of common law fraud—s*ee, e.g.*, Hanger Prosthetics & Orthotics, Inc. v. Capstone Orthopedic, Inc., 556 F. Supp. 2d 1122, 1131 (E.D. Cal. 2008) ("The term 'defraud' for purposes of § 1030(a)(4) simply means wrongdoing and does not require proof of common law fraud.")—namely "(1) a representation; (2) its falsity; (3) its materiality; (4) the speaker's knowledge of its falsity or ignorance of its truth; (5) an intent that it be acted on by the person and in the manner reasonably contemplated; (6) the hearer's ignorance of its falsity; (7) reliance on its truth; (8) the right to rely thereon; and (9) consequent and proximate injury." Wilcox v. First Interstate Bank of Or., NA, 815 F.2d 522, 531 n.7 (9th Cir. 1987) (citing Rice v. McAlister, 519 P.2d 1263, 1265 (Or. 1974)).

[125] S. REP. NO. 99-432, at 10 (1986).

someone will be defrauded) and intends that those consequences should occur (i.e., he intends that someone should be defrauded)."[126]

There are two additional requirements to violate § 1030(a)(4). First, the government must prove that in accessing the protected computer, the defendant furthered the fraud.[127] In other words, the access must be "directly linked to the intended fraud."[128] Thus, § 1030(a)(4) does not govern frauds where computer use is incidental—for example where an individual simply uses the computer for record keeping or to "add up his potential 'take' from the [fraud]."[129] Second, the government must prove that the defendant obtained "anything of value."[130] That element is "easily met if the defendant obtained money, cash, or a good or service with measurable value."[131] However, merely obtaining information may not alone suffice.[132] In addition, at least one court has concluded that whatever is taken must be valuable not merely in the abstract, but specifically to the defendant "in light of a fraudulent scheme."[133] Computer use, in and of itself, may be a thing of value for the purposes of § 1030(a)(4), but only if that use is worth at least $5,000 a year.[134] Although the concept of computer use as a thing of value is underdeveloped in case law, a Senate Report accompanying the 1986 Amendment to the CFAA provides some indication that computer use may be a thing of value where it reduces computer availability that would otherwise generate revenue for the computer owner through usage fees paid by valid users.[135] Although some observers have suggested that this idea is outmoded given the modern prevalence of computers and the corresponding decrease in the value of computer use,[136] the DOJ has suggested that it may still be possible for computer use to meet the $5,000 threshold in the case of recurring or continuing use of an expensive computer.[137] In any event, the $5,000 threshold for fraud solely resulting in computer use is intended to "minimize[] the possibility that mere computer trespassing will be prosecuted as fraud."[138] As the same 1986 Senate Report observed, if every trespass were thought of as "an attempt to defraud a service provider of computer time," it would obliterate the distinction between § 1030(a)(4) and the CFAA provisions that prohibit trespass.[139] In practice, it is difficult to invoke § 1030(a)(4) against a computer trespasser in the absence of other conduct, because courts may be reluctant to infer adequate proof of an intent to defraud from mere unauthorized computer access or even observation of data.[140]

---

[126] *See* Doyle, *supra* note 23, at 50.

[127] 18 U.S.C. § 1030(a)(4).

[128] S. REP. NO. 99-432, at 9 (1986).

[129] *Id.*

[130] 18 U.S.C. § 1030(a)(4).

[131] U.S. DEP'T OF JUSTICE, *supra* note 9, at 32.

[132] United States v. Czubinski, 106 F.3d 1069, 1078–79 (1st Cir. 1997) (reversing defendant's § 1030(a)(4) conviction for obtaining information because the "[t]he value of information is relative to one's needs and objectives" and "the government had to show that the information was valuable to [the defendant] in light of a fraudulent scheme").

[133] *Id.* at 1078.

[134] 18 U.S.C. § 1030(a)(4).

[135] S. REP. NO. 99-432, at 10 (1986) ("The Committee agrees that the mere use of a computer or computer service has a value all its own. Mere trespasses onto someone else's computer system can cost the system provider a 'port' or access channel that he might otherwise be making available for a fee to an authorized user.").

[136] KERR, *supra* note 7, at 99.

[137] U.S. DEP'T OF JUSTICE, *supra* note 9, at 32.

[138] *See* Doyle, *supra* note 23, at 51.

[139] S. REP. NO. 99-432, at 10 (1986).

[140] *Czubinski*, 106. F3d at 1075 (concluding that government did not adequately prove "intent to deprive . . . and, *a*

Damaging a Computer, 1030(a)(5)

Broadly speaking, § 1030(a)(5)[141] prohibits a variety of acts that result in damage to a computer. Subsection 1030(a)(5) may be used to prosecute many of the activities that are commonly associated with hacking, such as the transmission of viruses or worms and unauthorized access by intruders who delete files or shut off computers.[142] The provision may also be used to prosecute the perpetrators of Distributed Denial of Service (DDoS) attacks,[143] which occur, for example, when an attacker overwhelms a server's ability to process legitimate requests by overloading the server with a flood of illegitimate traffic.[144] Indeed, the government has invoked § 1030(a)(5) in a variety of prosecutions, such as those of a Russian national for deploying malware that "resulted in tens of millions of dollars of losses to victims worldwide";[145] an Illinois resident for developing websites used to launch "millions of DDoS attacks that disrupted the internet connections of targeted victim computers";[146] and the former IT employee of a major railroad who damaged his employer's computer network by "strategically delet[ing] files, remov[ing] administrative-level accounts, and chang[ing] passwords."[147]

The first act that § 1030(a)(5)—specifically under subsection (A)—criminalizes is to "knowingly cause[] the transmission of a program, information, code, or command" and thereby "intentionally cause[] damage without authorization, to a protected computer."[148] Transmission "encompasses a range of hacking activities, such as '[t]he transfer of operation or confidential information,' 'malicious software updates,' 'code injection attacks,' DDoS, and the 'embedding of malicious code' or malware."[149] Transmission may occur through use of the internet or physical

fortiori, a scheme to defraud" where defendant accessed computer and looked at confidential information, but there was no evidence that defendant intended to use that information for anything other than browsing).

[141] 18 U.S.C. § 1030(a)(5) imposes criminal liability on:

> (a) Whoever--
>
> > (5)(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;
> >
> > (B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
> >
> > (C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.

[142] U.S. DEP'T OF JUSTICE, *supra* note 9, at 35.

[143] *Id.*

[144] Cybersec. & Infrastructure Sec. Agency, *Security Tip (ST04-015): Understanding Denial-of-Service Attacks* (last revised Nov. 20, 2019), https://us-cert.cisa.gov/ncas/tips/ST04-015.

[145] Press Release, U.S. Dep't of Justice, Russian National Charged with Decade-Long Series of Hacking and Bank Fraud Offenses Resulting in Tens of Millions in Losses and Second Russian National Charged with Involvement in Deployment of "Bugat" Malware (Dec. 5, 2019), https://www.justice.gov/opa/pr/russian-national-charged-decade-long-series-hacking-and-bank-fraud-offenses-resulting-tens (quoting statement of Assistant Attorney General Brian A. Benczkowski).

[146] Press Release, U.S. Dep't of Justice, Former Operator of Illegal Booter Services Sentenced for Conspiracy to Commit Computer Damage and Abuse (Nov. 15, 2019), https://www.justice.gov/opa/pr/former-operator-illegal-booter-services-sentenced-conspiracy-commit-computer-damage-and-abuse.

[147] Press Release, U.S. Dep't of Justice, Former IT Employee of Transcontinental Railroad Sentenced to Prison for Damaging Ex-Employer's Computer Network (Feb. 13, 2018), https://www.justice.gov/opa/pr/former-it-employee-transcontinental-railroad-sentenced-prison-damaging-ex-employer-s-computer.

[148] 18 U.S.C. § 1030(a)(5)(A).

[149] Beale, *supra* note 1, at 170 (quoting Ioana Vasiu & Lucian Vasiu, *Break on Through: An Analysis of Computer Damage Cases*, 14 U. PITT. J. TECH. L. POL'Y 158, 167–69 (2014)).

mediums like compact discs.[150] Indeed, some courts have gone so far as to conclude that the exact means of transmission is actually irrelevant, focusing instead on whether the program, information, code, or command caused damage.[151] The phrase "program, information, code, or command" meanwhile, broadly includes "all transmissions that are capable of having an effect on a computer's operation," such as worms, "software commands (such as an instruction to delete information)," and "network packets designed to flood a network connection or exploit system vulnerabilities."[152]

To prove a § 1030(a)(5)(A) violation, the government must establish dual intents on the part of the defendant. First, the government must prove that the defendant's transmission was knowing.[153] That requirement excludes accidental transmission—for example, in the case of an unsuspecting user who recklessly or negligently forwards an email with malware attached in a file or link.[154] Second, the government must prove that the defendant intentionally caused damage to a protected computer without authorization.[155] The meanings of protected computer and without authorization are discussed in detail above, but the meaning of intent to cause damage requires further discussion. According to at least one court, intent in the context of § 1030(a)(5)(A) means that the defendant had the "conscious purpose of causing damage . . . to [the relevant] computer."[156] The CFAA defines damage to mean "impairment to the integrity or availability of data, a program, a system, or information,"[157] which occurs, for example, where a hacker causes a computer to behave in a manner contrary to the intentions of its owner.[158] Thus, an act that causes damage under the CFAA may include "clearly destructive behavior such as using a virus or worm or deleting data . . . [b]ut it may also include less obviously invasive conduct, such as flooding an email account."[159] For example, one federal court concluded that damage occurred as a result of

[150] Beale, *supra* note 1, at 170 (citing Deborah F. Buckman, Annotation, *Validity, Construction, and Application of Computer Fraud and Abuse Act (18 U.S.C.A. § 1030)*, 174 A.L.R. FED. 101 (2001)); *accord* United States v. Sullivan, 40 F. App'x 740, 743–44 (4th Cir. 2002) (per curiam) (concluding that a transmission under 18 U.S.C. § 1030(a)(5)(A) occurred through insertion of code into a computer system that eventually found its way into hand-held computers); N. Tex. Preventive Imaging LLC v. Eisenberg, No. SA CV 96-71AHS(EEX), 1996 WL 1359212, at *6 (C.D. Cal. Aug. 19, 1996) ("The transmission of a disabling code by floppy computer disk may fall within . . . [§ 1030(a)(5)(A)], if accompanied by the intent to cause harm.").

[151] *See, e.g.*, Patrick Patterson Custom Homes, Inc. v. Bach, 586 F. Supp. 2d 1026, 1035 (N.D. Ill. 2008) ("While Plaintiffs acknowledge that the precise method of installation of the erasure program is unknown, the Seventh Circuit recognizes that the precise mode of transmission is irrelevant.").

[152] U.S. DEP'T OF JUSTICE, *supra* note 9, at 37.

[153] 18 U.S.C. § 1030(a)(5)(A).

[154] *See* QVC, Inc. v. Resultly, LLC, 99 F. Supp. 3d 525, 536 (E.D. Pa. 2015) (concluding that § 1030(a)(5)(A) requires showing that "defendant intended to cause harm" and that "[d]amage caused by mere recklessness or negligence is insufficient").

[155] 18 U.S.C. § 1030(a)(5)(A).

[156] Pulte Homes, Inc. v. Laborers' Int'l Union of N. Am., 648 F.3d 295, 303 (6th Cir. 2011); *accord* United States v. Carlson, 209 F. App'x 181, 184 (3d Cir. 2006) (discussing § 1030(a)(5) prosecution and noting that although CFAA does not define "intentionally," "this Court has defined it in the criminal context as performing an act deliberately and not by accident").

[157] 18 U.S.C. § 1030(e)(8).

[158] *See* Berris, *supra* note **Error! Bookmark not defined.**, at 2 (explaining that damage "occurs, for example, where a hacker causes a computer to behave in a manner contrary to the intentions of its owner."); *accord* United States v. Yücel, 97 F. Supp. 3d 413, 420 (S.D.N.Y. 2015) (construing damage under § 1030(a)(5) to include instances where a computer is caused to "no longer operate[] only in response to the commands of the owner"). For a more detailed examination of different examples of damage, see, e.g., KERR, *supra* note 7, at 107–08.

[159] United States v. Hutchins, 361 F. Supp. 3d 779, 794 (E.D. Wis. 2019) (alterations in original) (quoting Fidlar Tech. v. LPS Real Estate Data Sols., Inc., 810 F.3d 1075, 1084–85 (7th Cir. 2016)).

an orchestrated effort to bombard a company's "sales offices and three of its executives with thousands of phone calls and e-mails," which diminished the ability of that company to use their systems.[160]

Other violations of § 1030(a)(5) may occur where a defendant intentionally accesses a protected computer without authorization and causes damage, even if he does not intend to cause such damage.[161] However, for such unintended damage to amount to a § 1030(a)(5) violation, it must either be reckless or result in loss.[162] Although the CFAA does not define what it means to recklessly cause damage, in general the "normal meaning of reckless in the criminal law (unlike the civil law) is that the defendant disregarded 'a risk of harm of which he is aware.'"[163] Although case law provides few illustrations, an individual may recklessly cause damage to a computer if he is aware of the risk that his unauthorized computer access may cause damage, but proceeds anyway and does indeed damage the computer.[164] The CFAA defines loss as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service."[165] Federal courts disagree on whether proving interruption of service—such as computer systems or files being rendered unavailable—is a prerequisite to demonstrating loss.[166] In other words, some courts construe loss to include reasonable costs caused by offenses regardless of whether those offenses involve service interruption, but other courts more narrowly interpret loss under the CFAA as requiring service interruption.[167]

[160] *Pulte Homes, Inc.*, 648 F.3d at 299, 301.

[161] 18 U.S.C. § 1030(a)(5).

[162] *Id.*

[163] United States v. McCord, Inc., 143 F.3d 1095, 1098 (8th Cir. 1998) (quoting Farmer v. Brennan, 511 U.S. 825, 837 (1994)).

[164] For example, one federal court found that a plaintiff sufficiently alleged a civil § 1030(a)(5) violation with allegations that the defendant recklessly caused damage by unauthorized computer access where he deleted data from the plaintiff's website, accounts, and server. MSC Safety Sols., LLC v. Trivent Safety Consulting, LLC, No. 19-CV-00938-MEH, 2019 WL 5189004, at *4 (D. Colo. Oct. 15, 2019).

[165] 18 U.S.C. § 1030 (e)(11). For a detailed examination of "loss," see, e.g., KERR, *supra* note 7, at 120–25.

[166] *See, e.g.*, Brown Jordan Int'l, Inc. v. Carmicle, 846 F.3d 1167, 1173–74 (11th Cir. 2017) (comparing jurisdictions that construe loss broadly to include any costs of responding to an offense regardless of whether there was an interruption of service with those that narrowly construe loss as resulting only from an interruption of service).

[167] *Compare id.* (adopting broad view of loss that includes reasonable costs of responding to an offense even where there was no interruption of service) *and* Yoder & Frey Auctioneers, Inc. v. EquipmentFacts, LLC, 774 F.3d 1065, 1073 (6th Cir. 2014) (holding that loss under the CFAA includes both consequential damages caused by service interruption and reasonable costs of responding to an offense such as damage assessments) *with* Gen. Sci. Corp. v. SheerVision, Inc., No. 10-CV-13582, 2011 WL 3880489, at *4 (E.D. Mich. Sept. 2, 2011) ("The CFAA only covers lost revenue if the loss occurred as a result of interrupted service.") *and* CoStar Realty Info., Inc. v. Field, 737 F. Supp. 2d 496, 515 (D. Md. 2010) ("[A] violation of the CFAA must cause an interruption of service in order for lost revenue to constitute as a qualifying 'loss' under the statute.").

Password Trafficking, 18 U.S.C. § 1030(a)(6)

Section 1030(a)(6)[168] is an "infrequently" used[169] section of the CFAA designed to protect computer passwords. The provision is "aimed at penalizing conduct associated with 'pirate bulletin boards,' where passwords are displayed that permit unauthorized access to others' computers."[170] Specifically, the law, assuming an appropriate jurisdictional nexus discussed below, makes it a crime to traffic "knowingly and with intent to defraud" in "any password or similar information through which a computer may be accessed without authorization."[171] For the purposes of § 1030(a)(6), "traffic" means to "transfer, or otherwise dispose of, to another, or obtain control of with intent to transfer or dispose of."[172] A defendant need not intend to profit to engage in trafficking for § 1030(a)(6) purposes, but he must intend to transfer or dispose of the passwords or similar information.[173] "Knowingly with intent to defraud" has the identical meaning as in § 1030(a)(4), discussed above, and generally refers to acts undertaken with the knowledge that defrauding another is a likely consequence, and the intent that such fraud should actually occur.[174] "Password[s] or similar information"[175] is a broad category intended to include not "only a single word that enables one to access a computer," but also "longer more detailed explanations on how to access others' computers."[176]

For § 1030(a)(6) to apply, the defendant's actions must satisfy one of two jurisdictional hooks. First, § 1030(a)(6) could apply where the "trafficking affects interstate or foreign commerce."[177] Although undefined by the CFAA and underdeveloped in case law, at least some courts examining civil § 1030(a)(6) claims appear to have construed the interstate or foreign commerce requirement broadly.[178] For example, for at least one court, trafficking involving the internet could satisfy the requirement.[179] Second, § 1030(a)(6) may also apply where the defendant traffics in passwords or similar information that would allow unauthorized entry into a "computer . . . used by or for the Government of the United States."[180] Again there is no statutory definition

---

[168] 18 U.S.C. § 1030(a)(6) imposes criminal liability on:

> (a) Whoever--
>
> > (6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if--
> >
> > > (A) such trafficking affects interstate or foreign commerce; or
> >
> > > (B) such computer is used by or for the Government of the United States.

[169] *See* Doyle, *supra* note 23, at 69.

[170] S. REP. NO. 99-432, at 13 (1986).

[171] 18 U.S.C. § 1030(a)(6).

[172] *Id.* § 1029(e)(5); *see id.* § 1030.

[173] U.S. DEP'T OF JUSTICE, *supra* note 9, at 50.

[174] *See supra* § "Computer Fraud: 18 U.S.C. § 1030(a)(4)."

[175] 18 U.S.C. § 1030(a)(6).

[176] S. REP. NO. 99-432, at 13 (1986); *accord* U.S. DEP'T OF JUSTICE, *supra* note 9, at 50 ("Therefore, prosecutors should apply the term 'password' using a broad meaning to include any instructions that safeguard a computer.").

[177] 18 U.S.C. § 1030(a)(6)(A).

[178] *See* Tracfone Wireless, Inc. v. Simply Wireless, Inc., 229 F. Supp. 3d 1284, 1297 (S.D. Fla. 2017) (concluding that plaintiff stated claim under § 1030(a)(6) where trafficking implicated the internet and a telecommunications network).

[179] *Id.* Courts have reached similar conclusions when interpreting 18 U.S.C. § 1029, a credit card fraud statute that prohibits trafficking that "affects interstate or foreign commerce." *See, e.g.*, United States v. Rushdan, 870 F.2d 1509, 1513–14 (9th Cir. 1989) (concluding that federal jurisdiction under § 1029 included "possession of the numbers of out of state credit card accounts").

[180] 18 U.S.C. § 1030(a)(6)(B).

and little interpretive case law, but according to the DOJ the "plain meaning [of the phrase] should encompass any computer used for official business by a federal government employee or on behalf of the federal government."[181] However, it is at least possible that the provision only applies to passwords for executive branch agencies.[182] That is because unlike other CFAA provisions, § 1030(a)(6) does not specify that a government computer is one used by any "department or agency of the United States" a phrase that the CFAA specifically defines as including legislative, executive, and judicial branch computers.[183] Thus, it has been theorized that the use in § 1030(a)(6) of the phrase "computer . . . . used by or for the Government of the United States" might carry a meaning narrower than the phrase "computer[s] of a department or agency of the United States" used elsewhere in the CFAA.[184]

Threats and Extortion, 18 U.S.C. § 1030(a)(7)

Section 1030(a)(7)[185] prohibits certain extortionate threats concerning a protected computer, such as threats to cause damage to, or disclose confidential information from, a protected computer unless paid.[186] The provision has been described as "a high-tech variation on old fashioned extortion."[187] Although a number of other federal criminal statutes also prohibit extortionate threats, the CFAA's legislative history suggest that Congress's concern in enacting this provision was that other "extortion statutes, which protect against physical injury to person or property, [might not] cover intangible computerized information."[188] In particular, the Senate Report accompanying the 1996 Amendment to the CFAA noted concern with threats against computer systems such as "situations in which hackers penetrate a system, encrypt a database and then demand money for the decoding key."[189] Prosecutors have invoked § 1030(a)(7) to charge a variety of threats against computer systems themselves, such as ransomware plots that use software to encrypt the victim's computer files (rendering them unavailable) until payment is received to unlock those systems.[190] The government has also relied on § 1030(a)(7) to prosecute

[181] U.S. DEP'T OF JUSTICE, *supra* note 9, at 51.

[182] *See* Doyle, *supra* note 23, at 69–70 ("[I]t is unclear whether the protection of paragraph 1030(a)(6) cloaks legislative and judicial branch computers or is limited to those of the executive branch.").

[183] 18 U.S.C. § 1030(e)(7) ("[T]he term 'department of the United States' means the legislative or judicial branch of the Government or one of the executive departments . . . .").

[184] Doyle, *supra* note 23 (quoting (18 U.S.C. § 1030)).

[185] 18 U.S.C. § 1030(a)(7) imposes criminal liability on:

> (a) Whoever--
>
> > (7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any--
> >
> > > (A) threat to cause damage to a protected computer;
> >
> > > (B) threat to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; or
> >
> > > (C) demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion.

[186] *Id.*

[187] *See* S. REP. NO. 104-357, at 12 (1996).

[188] *Id.* (quoting statement of Attorney General to Sen. Leahy).

[189] *Id.*

[190] *See, e.g.*, Indictment, United States v. Savandi, No. 3:18-cr-00704-BRM, 2018 WL 6798078 (D.N.J. Nov. 27, 2018); Press Release, U.S. Dep't of Justice, Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million in Losses (Nov. 28, 2018),

instances where computers are not the subject of the threat, but rather the means of extortion. For instance, prosecutors have brought charges under § 1030(a)(7) against a hacker who obtained "sensitive records and information" from victim computers, which he threatened to release unless paid a ransom.[191] As another illustration, federal prosecutors invoked § 1030(a)(7) in charging a former government employee who used stolen passwords to obtain "sexually explicit photographs . . . from victims' email and social media accounts," which he "threatened to share . . . unless the victims ceded to certain demands."[192]

Section 1030(a)(7) specifically prohibits three categories of extortionate threats. First, it criminalizes "threat[s] to cause damage to a protected computer."[193] Threats to cause damage might include threats to "interfer[e] in any way with the normal operation of the computer or system in question, such as [by] denying access to authorized users, erasing or corrupting data or programs, slowing down the operation of the computer or system, or encrypting data and then demanding money for the key."[194] Second, § 1030(a)(7) proscribes "threat[s] to obtain information from a protected computer without authorization or in excess of authorization *or* to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access."[195] In other words, this second category includes extortionate threats to obtain information through unauthorized access to a protected computer, *or* to disclose information *already obtained* through unauthorized access into a protected computer.[196] For example, an individual may fall within this second category when he hacks into a protected computer, obtains sensitive information, and then threatens to disclose it unless his demands are met.[197] Third, it is a crime under § 1030(a)(7) to "demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion."[198] An example of this type of threat is the use of ransomware to extort payment in exchange for providing the decryption key for the victim's files.[199] The latter two categories of threats are intended to "'cover the situation in which a criminal has already stolen the information and threatens to disclose it unless paid off' and in which 'other criminals

https://www.justice.gov/opa/pr/two-iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public. The installation of such ransomware may also violate § 1030(a)(5). *See* Indictment, *Savandi*, No. 3:18-cr-00704-BRM, 2018 WL 6798078, *supra* note 190 (charging defendants under both 18 U.S.C. § 1030(a)(7)(C) and § 1030(a)(5)(A)).

[191] Press Release, U.S. Dep't of Justice, Member of "The Dark Overlord" Hacking Group Extradited From United Kingdom to Face Charges in St. Louis (Dec. 18, 2019), https://www.justice.gov/opa/pr/member-dark-overlord-hacking-group-extradited-united-kingdom-face-charges-st-louis. *See also* Indictment, United States v. Wyatt, No. 4:17-cr-00522-RLW-SPM, 2017 WL 11530077 (E.D. Mo. Nov. 8, 2017).

[192] Press Release, U.S. Dep't of Justice, Former U.S. Government Employee Charged in Computer Hacking and Cyber Stalking Scheme (Aug. 19, 2015), https://www.justice.gov/opa/pr/former-us-government-employee-charged-computer-hacking-and-cyber-stalking-scheme; *see also* Indictment, United States v. Ford, No. 1 15-CR-319, 2015 WL 4980336 (N.D. Ga. Aug. 18, 2015).

[193] 18 U.S.C. § 1030(a)(7)(A).

[194] *See* S. REP. NO. 104-357, at 12 (1996).

[195] 18 U.S.C. § 1030(a)(7)(B) (emphasis added).

[196] *Id.*

[197] Indictment, *Ford*, No. 1 15-CR-319, 2015 WL 4980336, *supra* note 192.

[198] 18 U.S.C. § 1030(a)(7)(C).

[199] U.S. DEP'T OF JUSTICE, *supra* note 9, at 54; *accord* S. REP. NO. 104-357, at 12 (1996) (discussing § 1030(a)(7) and noting that "[o]ne can imagine situations in which hackers penetrate a system, encrypt a database and then demand money for the decoding key").

cause damage first—such as by accessing a corporate computer without authority and encrypting critical data—and then threaten that they will not correct the problem unless the victim pays.'"[200]

There are two important limitations to § 1030(a)(7) as it pertains to all three categories of threats, however. First, for § 1030(a)(7) to apply, the defendant must have acted "with intent to extort from any person any money or other thing of value."[201] In general, extortion refers to "obtaining something or compelling some action by illegal means, as by force or coercion."[202] In the context of § 1030(a)(7), courts have found the requisite intent to extort where, for example, defendants wrongfully obtained confidential information or credentials and demanded money for their return.[203] However, it may not be necessary to establish "that the defendant actually succeeded in obtaining the money or thing of value, or that the defendant actually intended to carry out the threat made."[204] Second, the defendant must have transmitted the threat "in interstate or foreign commerce,"[205] for example by transmitting the threat through the internet or between computers in two different states.[206]

Remedies and Penalties

The CFAA provides a number of remedies when its various prohibitions are violated. Most obviously, violations of the CFAA provisions discussed above are subject to various criminal penalties of fines and imprisonment.[207] The nature of those penalties varies based on the specific subsection at issue (*see* **Table 1**).[208] For example, the maximum prison term for first-time CFAA offenders is one year under § 1030(a)(3),which governs certain act of trespassing in government computers,[209] but five years under § 1030(a)(4), which is the main anti-fraud provision in the CFAA and which ordinarily involves conduct of a more serious nature.[210] The distinction between first time and repeat offenses is also relevant in the CFAA (*see* **Table 1**). For instance, under §

[200] *See* Doyle, *supra* note 23, at 63 & n. 353 (quoting *H.R. 4175, the Privacy and Cybercrime Enforcement Act of 2007: Hearings Before the Subcomm. on Crime, Terrorism, and Homeland Security of the House Comm. on the Judiciary*, 110th Cong., 1st Sess. (2007) (statement of Acting Principal Deputy Assistant Attorney General Andrew Lourie)).

[201] 18 U.S.C. § 1030(a)(7).

[202] *Extortion*, BLACK'S LAW DICTIONARY (11th ed. 2019).

[203] *See, e.g.*, Inplant Enviro-Sys. 2000 Atlanta, Inc. v. Lee, No. 1:15-CV-0394-LMM, 2015 WL 13297963, at *4 (N.D. Ga. June 9, 2015) (holding that plaintiff alleged a valid claim for § 1030(a)(7) violation where defendant allegedly demanded $137,705 for the return of master access to the plaintiff's domains).

[204] U.S. DEP'T OF JUSTICE, *supra* note 9, at 53.

[205] 18 U.S.C. § 1030(a)(7).

[206] *See Inplant Enviro-Sys. 2000 Atlanta, Inc.*, No. 1:15-CV-0394-LMM, 2015 WL 13297963, at *4 (concluding that plaintiff adequately stated a § 1030(a)(7) violation against defendant who transmitted extortionate communication "in interstate or foreign commerce, as [it was] sent via internet . . . ."); *accord* United States v. Kammersell, 196 F.3d 1137, 1139 (10th Cir. 1999) (concluding in that interstate commerce element of 18 U.S.C. § 875(c)—a federal threat statute—was satisfied where defendant transmitted threat via instant message between computers in the same state, where it was routed to a server in a second state).

[207] 18 U.S.C. § 1030. The CFAA gives the FBI "primary authority to investigate" certain CFAA violations such as those involving espionage or national security information, but the statute also expressly permits investigation by the United States Secret Service and any other agency with authority. 18 U.S.C. § 1030(d); *accord* FBI, *Cyber Crime*, https://www.fbi.gov/investigate/cyber (last visited July 27, 2020). The Department of Justice prosecutes CFAA violations. *See generally* U.S. DEP'T OF JUSTICE, *supra* note 9 (summarizing DOJ policies and guidance on CFAA prosecutions).

[208] 18 U.S.C. § 1030.

[209] *Id.* § 1030(c)(2)(A).

[210] *Id.* § 1030(c)(3)(A).

1030(a)(1)—which prohibits obtaining and disclosing national security information through unauthorized computer access—a violation is generally subject to a maximum prison term of ten years, a fine, or both.[211] But if that violation occurs after another CFAA offense, it is subject to a maximum prison term of twenty years, a fine, or both.[212] Within some CFAA provisions, the relevant penalties also depend on the gravity of the defendant's conduct (*see* **Table 2**; **Table 3**; **Table 4**). For example, under § 1030(a)(2)—prohibiting obtaining information in certain circumstances—the penalties are stiffer if the value of the information obtained is greater than $5,000 (*see* **Table 2**).[213] The CFAA provision prohibiting damage to computers—§ 1030(a)(5)—offers another illustration (*see* **Table 3**; **Table 4**). It authorizes longer prison terms for certain outcomes, such as when a violation results in bodily injury or death.[214]

Table 1. Overview of CFAA Maximum Penalties

Maximum Prison Terms by Subsection for First and Subsequent Offenses

Section*	Description	First Offense**	Subsequent Offense***
1030(a)(1)	Cyber Espionage	10 Years	20 Years
1030(a)(2)	Obtaining Information by Unauthorized Computer Access	1 Year (M); 5 Years (F)	10 Years
1030(a)(3)	Government Computer Trespassing	1 Year	10 Years
1030(a)(4)	Computer Fraud	5 Years	10 Years
1030(a)(5)(A)	Knowing Transmission + Intentional Damage to Computer	1 Year (M); 10 Years (F)	20 Years
1030(a)(5)(B)	Intentional Access + Reckless Damage to Computer	1 Year (M); 5 Years (F)	20 Years
1030(a)(5)(C)	Intentional Access + Damage to Computer + Loss	1 Year	10 Years
1030(a)(6)	Password Trafficking	1 Year	10 Years
1030(a)(7)	Threats and Extortion	5 Years	10 Years

Source: 18 U.S.C. § 1030(c).

Notes:

* Bolded subsection authorizes additional penalties beyond those reflected in this Table where there are certain aggravating factors such as causing death, broken down in further detail in **Table 3**.

** (M) denotes misdemeanor; (F) denotes felony. CFAA subsections that may be charged as a misdemeanor or a felony are broken down in further detail in **Table 2**, **Table 3**, and **Table 4**.

*** Subsequent offense refers to maximum penalties possible for offense committed following conviction for another CFAA offense.

[211] *Id.* § 1030(c)(1)(A).

[212] *Id.* § 1030(c)(1)(B).

[213] *Id.* § 1030(c)(2)(B).

[214] *Id.* §§ 1030(c)(4)(E)–(F).

Table 2. Overview of Maximum Penalties Under 18 U.S.C. § 1030(a)(2)

Maximum Prison Terms for Obtaining Information by Unauthorized Computer Access

Description of Offense Under § 1030(a)(2)	Classification	Sentence
First Offense (No Special Conditions)	Misdemeanor	1 Year
Offense with One of Three Special Conditions: 1. Offense committed for purpose of commercial advantage or private financial gain; 2. Offense committed in furtherance of any criminal or tortious act in violation of the Constitution or state or federal law; or 3. The Value of the information obtained is greater than $5,000.	Felony	5 Years
Subsequent Offense*	Felony	10 Years

Source: 18 U.S.C. § 1030(c)(2)(C).

Note: * Subsequent offense refers to maximum penalties possible for offense committed following conviction for another CFAA offense.

Table 3. Overview of Maximum Penalties Under 18 U.S.C. § 1030(a)(5)(A)

Maximum Prison Terms for Knowing Transmission + Intentional Damage to a Computer

Description of Offense Under § 1030(a)(5)(A)	Classification	Sentence
First Offense (No Special Harms)	Misdemeanor	1 Year
First Offense with One of Six Special Harms: 1. Minimum loss of $5,000 to at least one person during a one year period; 2. Modification/impairment/potential modification or impairment of medical examination, diagnosis, treatment, or care of at least one individual; 3. Physical injury to any person; 4. Threat to public health or safety; 5. Damage affecting a computer used by or for the federal government in furtherance of the administration of justice, national defense, or national security; or 6. Damage affecting at least 10 protected computers in a 1-year period.	Felony	10 Years
Subsequent Offense*	Felony	20 Years
Offense where defendant knowingly/recklessly causes serious bodily injury, or attempts to do so	Felony	20 Years
Offense where defendant knowingly/recklessly causes death, or attempts to do so	Felony	Life Imprisonment

Source: 18 U.S.C. § 1030(c)(4).

Note: * Subsequent offense refers to maximum penalties possible for offense committed following conviction for another CFAA offense.

Table 4. Overview of Maximum Penalties Under 18 U.S.C. § 1030(a)(5)(B)

Maximum Prison Terms for Intentional Access + Reckless Damage to a Computer

Description of Offense Under § 1030(a)(5)(B)	Classification	Sentence
First Offense (No Special Harms)	Misdemeanor	1 Year
First Offense with One of Six Special Harms: 1. Minimum loss of $5,000 to at least one person during a one year period; 2. Modification/impairment/potential modification or impairment of medical examination, diagnosis, treatment, or care of at least one individual; 3. Physical injury to any person; 4. Threat to public health or safety; 5. Damage affecting a computer used by or for the federal government in furtherance of the administration of justice, national defense, or national security; or 6. Damage affecting at least 10 protected computers in a 1-year period.	Felony	5 Years
Subsequent Offense*	Felony	20 Years

Source: 18 U.S.C. § 1030(c)(4).

Note: * Subsequent offense refers to maximum penalties possible for offense committed following conviction for another CFAA offense.

In addition to these criminal penalties, the CFAA also provides a private right of action that permits a person who suffers damage or loss due to a CFAA violation to bring suit against the violator. Under a civil CFAA claim, the plaintiff can obtain compensatory damages and injunctive relief or other equitable relief.[215] However, civil actions are only possible if the violation results in certain types of losses or damages, such as physical injury, a threat to public health or safety, damage to 10 or more protected computers within the span of a year, or certain losses with a total value of at least $5,000.[216] Finally, the CFAA includes forfeiture provisions that authorize government confiscation of property that was used in, or derived from, CFAA violations.[217]

Selected CFAA Issues in the 116th Congress

The CFAA exists in the larger context of a rapidly changing technological world. Such changes have made the application of the CFAA to certain activities uncertain and even controversial. For example, with the modern prevalence of cybercrime, some contend that private actors who fall victim to cyberattacks should be able to hack back against the initial aggressor.[218] However, the provisions of the CFAA that prohibit hacking also ostensibly criminalize hacking back, which

[215] *Id.* § 1030(g).

[216] *Id.* § 1030(c)(4)(A)(i). A complete examination of these requirements, and the CFAA's civil remedy more broadly, is beyond the scope of this Report. For a more detailed examination, see Doyle, *supra* note 23.

[217] *Id.* § 1030(j). A more detailed examination of the laws governing forfeiture is beyond the scope of this Report. For an analysis of forfeiture, including under § 1030, see CRS Report 97-139, *Crime and Forfeiture*, by Charles Doyle.

[218] *See infra* § "Hacking Back."

some legislation has sought to change.[219] Another technological development that has prompted reexamination of the CFAA by some policymakers involves the growing market for the sale and rental of botnets: "network[s] of compromised computers, 'often programmed to complete a set of repetitive tasks' without 'the owner's knowledge or permission.'"[220] Although the CFAA generally criminalizes creating botnets or using them for other computer crimes, it may not prohibit the sale or renting of botnets.[221] The proliferation of Terms of Service (ToS) Agreements—contracts that govern the use of a product such as a website—has resulted in another area of uncertainty under the CFAA.[222] Specifically, federal courts disagree over whether the CFAA imposes criminal liability for ToS violations.[223] This section discusses the CFAA in relation to each of these examples of the intersection between technological change and the law.

The CFAA and ToS Violations

One ongoing issue with respect to the CFAA is whether the statute imposes criminal liability for the bare violations of ToS agreements—contracts that govern the use of a product.[224] The issue is of considerable significance given the prevalence of ToS agreements, which frequently govern the use of smartphones, tablets, personal computers, social media websites, apps, online shopping platforms, streaming services, and more.[225] The countervailing policy concerns are the danger of over criminalization on the one hand, versus the importance of enforcing ToS agreements on the other.[226]

Currently, there is an unresolved circuit split over whether the CFAA imposes criminal liability for ToS violations, as a result of conflicting interpretations of the breadth of the phrases "without authorization" and "exceeds authorized access." Several courts, including the U.S. Court of Appeals for the First,[227] Fifth,[228] Seventh,[229] and Eleventh[230] Circuits have interpreted "exceeds authorized access" and "without authorization" broadly, in a manner that would permit criminal liability for violations of ToS agreements and other contractual computer use restrictions. For example, in *United States v. Rodriguez*, the Eleventh Circuit[231] concluded that an employee

[219] *Id.*

[220] Beale, *supra* note 1, at 173 (quoting Zach Lerner, *Microsoft the Botnet Hunter: The Role of Public-Private Partnerships in Mitigating Botnets*, 28 HARV. J.L. & TECH. 237, 239 (2014)); *accord* United States v. Gasperini, 894 F.3d 482, 485 (2d Cir. 2018) (describing botnets as "network[s] of infected computers under the attacker's control.").

[221] *See infra* § "Botnet Trafficking."

[222] *See infra* § "The CFAA and ToS Violations."

[223] *Id.*

[224] Berris, *supra* note 14. More broadly, legal commentators have described this issue as whether the CFAA imposes criminal liability for the violation of "contract-based restrictions." KERR, *supra* note 7, at 51.

[225] Berris, *supra* note 14.

[226] *Id.*

[227] EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58, 62 (1st Cir. 2003) ("A lack of authorization could be established by an explicit statement on the website restricting access.").

[228] United States v. John, 597 F.3d 263, 271 (5th Cir. 2010) (holding that authorized access may "encompass limits placed on *the use* of information obtained by permitted access to a computer system and data available on that system . . . at least when the user knows or reasonably should know that he or she is not authorized to access a computer and information obtainable from that access in furtherance of or to perpetrate a crime.")

[229] Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2006) (concluding that defendant lacked authorization after breaching duty of loyalty to employer).

[230] United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010) (concluding that defendant exceeded authorized access by violating employer policy against using employer database for personal purposes).

[231] This report references a significant number of decisions by federal appellate courts of various regional circuits. For

"exceeded authorized access" under the CFAA when he used a database he was authorized to access, but did so for personal purposes in a manner prohibited by his employer's computer use policy.[232] In other words, for the Eleventh Circuit, "the concept of 'exceeds authorized access' may include exceeding the purposes for which access is 'authorized.'"[233] In general, these courts view the CFAA to be concerned with not just hacking, but also with other computer-based harms such as the misappropriation of confidential information by rogue employees or former-employees.[234]

In contrast, several other courts, including the Second,[235] Fourth,[236] and Ninth[237] Circuits, have more narrowly interpreted "without authorization" and "exceeds authorized access," based on an understanding that the CFAA's central purpose is to criminalize hacking. These courts apply CFAA liability only to those who lack any authorization to access a computer or website[238] or those who are "authorized to access only certain data or files" but access "unauthorized data or files."[239] For example, under the narrow view, an employee with permission to access only product information on his employer's computer would exceed authorized access if he also looks at *customer data* on that computer, as he was wholly lacking authority to view the customer information.[240] But, if that employee were permitted to access customer data for certain reasons (e.g., business purposes) and he did so for other *purposes* (e.g., personal curiosity), under the narrow view, he would not have exceeded authorized access. Thus, courts applying the narrow view would generally exclude from CFAA liability those who have merely violated ToS agreements because those agreements generally do not restrict *access*, but rather restrict the *purposes* to which a database or computer may be used once it has been accessed.[241] Under this view, CFAA liability could only apply to such individuals if their permission to access a computer or website "has been revoked explicitly," such as through a cease and desist letter.[242] Courts adopting the narrow interpretation have expressed concern that a broad reading of "without authorization" and "exceeds authorized access" would risk defining authorized access by contract terms that "most people are only dimly aware of," and are subject to change without notice, risking "mak[ing] criminals of large groups of people who would have little reason to suspect they are committing a federal crime."[243] Adherents to the broad interpretation counter that

purposes of brevity, references to a particular circuit in the body of this report (e.g., the First Circuit) refer to the U.S. Court of Appeals for that particular circuit.

[232] *Rodriguez*, 628 F.3d at 1263.

[233] *John*, 597 F.3d at 272.

[234] Berris, *supra* note 14.

[235] United States v. Valle, 807 F.3d 508, 523 (2d Cir. 2015) (concluding that an individual does not exceed authorized access where individual is authorized for certain uses, and surpasses those).

[236] WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199, 206 (4th Cir. 2012) ("[W]e adopt a narrow reading of the terms 'without authorization' and 'exceeds authorized access' and hold that they apply only when an individual accesses a computer without permission or obtains or alters information on a computer beyond that which he is authorized to access.").

[237] United States v. Nosal, 676 F.3d 854, 863 (9th Cir. 2012) ("Instead, we hold that the phrase 'exceeds authorized access' in the CFAA does not extend to violations of use restrictions.").

[238] *See Valle*, 807 F.3d at 528.

[239] *Nosal*, 676 F.3d at 856–57.

[240] *Id.* at 857.

[241] Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1067 (9th Cir. 2016) ("Second, a violation of the terms of use of a website—without more—cannot establish liability under the CFAA.").

[242] *Id.*

[243] *Nosal*, 676 F.3d at 859, 861.

application of the CFAA is sufficiently tempered by, among other things, prosecutorial discretion and statutory intent requirements.[244]

The Supreme Court is currently considering a case that could resolve whether the CFAA imposes criminal liability for mere ToS violations. On April 20, 2020 the Court agreed to hear *Van Buren v. United States*,[245] an appeal from the Eleventh Circuit.[246] *Van Buren,* involves former police sergeant Nathan Van Buren's conviction for, among other things, violating § 1030(a)(2) by using a law enforcement database for purposes prohibited by department policy.[247] The Court is expected to hear arguments in *Van Buren* in its October 2020 term.[248]

And regardless of what the Court does in *Van Buren*, Congress could clarify the CFAA's reach with respect to ToS agreements. In past Congresses, legislation has been introduced that sought to modify the "without authorization" and "exceeds authorized access" language in the CFAA.[249] One example, Aaron's Law,[250] "[n]amed in honor of the late Internet innovator and activist Aaron Swartz,"[251] was introduced in the 113th Congress. Aaron's Law would have replaced the phrase "exceeds authorized access" with the phrase "access without authorization," defining the latter as obtaining "information on a protected computer . . . that the accesser lacks authorization to obtain" by "knowingly circumventing one or more technological or physical measures that are designed to exclude or prevent unauthorized individuals from obtaining that information."[252] That proposal would have limited the CFAA's breadth in a manner more consistent with the understanding of courts applying the narrow view of the statute. No bills have been introduced in this Congress addressing the split.

Botnet Trafficking

The role of the CFAA has also received attention in the context of botnets—"network[s] of compromised computers, 'often programmed to complete a set of repetitive tasks' without 'the owner's knowledge or permission.'"[253] Botnets pose a significant risk because they are sometimes used for attacks on the internet itself, for example in DDoS attacks against core internet infrastructure.[254] The creation of a botnet and the use of a botnet to commit crimes generally

[244] Berris, *supra* note 14.

[245] Van Buren v. United States, 206 L. Ed. 2d 822 (Apr. 20, 2020).

[246] United States v. Van Buren, 940 F.3d 1192 (11th Cir. 2019), *cert. granted*, No. 19-783, 2020 WL 1906566 (Apr. 20, 2020).

[247] *Id.* at 1197–98, 1208.

[248] *October Term 2020*, SCOTUSBLOG, https://www.scotusblog.com/case-files/terms/ot2020/?sort=mname (last visited Sept. 9, 2020).

[249] Aaron's Law Act of 2013, H.R. 2454, 113th Cong. (2013).

[250] *Id.*

[251] Press Release, U.S. Congresswoman Zoe Lofgren, Rep Zoe Lofgren Introduces Bipartisan Aaron's Law (June 20, 2013), https://lofgren.house.gov/media/press-releases/rep-zoe-lofgren-introduces-bipartisan-aarons-law.

[252] Aaron's Law Act of 2013, H.R. 2454, 113th Cong. (2013).

[253] Beale, *supra* note 1, at 173 (quoting Zach Lerner, *Microsoft the Botnet Hunter: The Role of Public-Private Partnerships in Mitigating Botnets*, 28 HARV. J.L. & TECH. 237, 239 (2014)); *accord* United States v. Gasperini, 894 F.3d 482, 485 (2d Cir. 2018) (describing botnets as "network[s] of infected computers under the attacker's control.").

[254] *See* Beale, *supra* note 1, at 190 ("In contrast, botnets present the reverse issue: devices connected to the internet may be used to disrupt the internet itself.").

violates the CFAA.[255] However, at times, individuals develop botnets that are rented or sold[256] to other individuals who, in turn, then use them for various crimes such as DDoS attacks and identity theft.[257] Federal courts have not resolved whether the CFAA criminalizes such botnet trafficking, and the issue is particularly uncertain in the case of botnets offered for rent or sale by individuals who did *not* also create them (the CFAA generally criminalizes the creation of a botnet).[258] For example, in a 2015 blog post the DOJ recounted one undercover investigation that revealed a seller offering a botnet comprised of thousands of computers; prosecutors were unable to bring charges against the seller because it was unclear whether he had created the botnet or was simply selling it.[259]

Thus, the DOJ has seemingly acknowledged that some botnet trafficking conduct may fall outside the scope of the CFAA.[260] A review of the language of the CFAA reveals the reason. The only CFAA provision that expressly prohibits trafficking—§ 1030(a)(6)—covers only passwords and related information, not botnets.[261] Another relevant CFAA subsection—§ 1030(a)(5)'s prohibition against damaging certain computers—requires that the defendant acts with intent to damage.[262] However, those trafficking in botnets might lack such intent, if they simply intend to profit or are unaware of how the botnet will be used.[263] Nevertheless, the DOJ has reached several plea agreements with defendants accused of botnet trafficking.[264] The counts included in those plea agreements have generally been some combination of conspiracy (under 18 U.S.C. § 371) to violate the CFAA or the wire fraud statute,[265] attempt to damage computers by transmission of programs, codes or commands in violation of the CFAA,[266] and "advertising a device used to intercept electronic communications" in violation of 18 U.S.C. § 2512.[267]

Although at first glance the conspiracy statute invoked by the DOJ in some such plea agreements appears like it could have widespread applicability in the context of botnet trafficking, a

---

[255] U.S. Dep't of Justice, *Prosecuting the Sale of Botnets and Malicious Software* (Mar. 18, 2015), https://www.justice.gov/archives/opa/blog/prosecuting-sale-botnets-and-malicious-software.

[256] *See* Matwyshyn, *supra* note 13, at 503 ("There are cases where brokers who sell access to botnets are not the criminals who created them.").

[257] U.S. Dep't of Justice, *Prosecuting the Sale of Botnets*, *supra* note 255.

[258] *Id.*; *accord* Triana, *supra* note 13, at 1315 (discussing uncertainty of whether sale of botnets and malware would violate the CFAA).

[259] U.S. Dep't of Justice, *Prosecuting the Sale of Botnets*, *supra* note 255.

[260] *See id.* ("While trafficking in botnets is sometimes chargeable under other subsections of the Computer Fraud and Abuse Act, [the problem of individuals trafficking in botnets that they did not create] has resulted in, and will increasingly result in, the inability to prosecute individuals selling access to thousands of infected computers.").

[261] 18 U.S.C. § 1030(a)(6).

[262] *Id.* § 1030(a)(5).

[263] *See* Triana, *supra* note 13, at 1315 ("Since hackers selling malware more clearly intend to profit off of their skills, they likely do not meet the mens rea requirement of 'intentionally' causing 'damage.'").

[264] *See, e.g.*, Press Release, U.S. Dep't of Justice, Marcus Hutchins Pleads Guilty to Creating and Distributing the Kronos Banking Trojan and UPAS Kit Malware (May 3, 2019), https://www.justice.gov/usao-edwi/pr/marcus-hutchins-pleads-guilty-creating-and-distributing-kronos-banking-trojan-and-upas.

[265] *Id.*; Press Release, U.S. Dep't of Justice, Russian Citizen Sentenced to 46 Months in Prison for Involvement in Global Botnet Conspiracy (Aug. 3, 2017), https://www.justice.gov/opa/pr/russian-citizen-sentenced-46-months-prison-involvement-global-botnet-conspiracy.

[266] *See* Press Release, U.S. Dep't of Justice, Arizona Man Sentenced to 30 Months in Prison for Selling Access to Botnets (Sept. 6, 2012), https://www.justice.gov/opa/pr/arizona-man-sentenced-30-months-prison-selling-access-botnets.

[267] *See* Press Release, *supra* note 264.

defendant is not guilty of conspiracy unless: (1) he has agreed to commit a specific offense with at least one other person; (2) he knowingly participated in the conspiracy while intending to commit that offense; and (3) a conspirator commits an overt act in furtherance of the conspiracy.[268] The second element—intent—likely presents a significant obstacle in some cases, because as discussed, botnet traffickers may be unaware of how the buyer or renter plans to use the botnet, and may be intending only to profit.[269] Thus, the seller may lack the requisite intent to commit an underlying offense.[270] And, for the reasons outlined above, botnet trafficking by itself does not appear to violate the CFAA and therefore would likely not amount to an underlying federal offense. Even in instances where the conspiracy statute does reach botnet trafficking—for example, if a botnet trafficker rents botnet access with the intent that it should be used to damage a computer in violation of § 1030(a)(5)—the statute authorizes a maximum prison term of five years,[271] less than under some subsections of the CFAA.[272]

At least one state has enacted a law aimed at botnet trafficking,[273] and the issue has generated legislative proposals in previous administrations[274] and Congress.[275] For example, one proposal introduced in the 116th Congress, titled the Defending American Security from Kremlin Aggression Act of 2019, contains a provision that would amend the CFAA to prohibit "intentionally traffic[king] in the means of access to a protected computer."[276] Although the proposal does not define "means of access," the intent appears to be to include botnets.[277] If enacted, the prohibition would be subject to two main limitations.[278] First, the trafficker must "know[] or [have] reason to know the protected computer has been damaged in a manner prohibited by" the CFAA.[279] Second, the trafficker must know or have reason to know that the purchaser or renter intends to use the means of access to violate certain laws or to "damage a protected computer" in violation of the CFAA.[280] The botnet trafficking provision of in this legislation is largely identical to a stand-alone botnet trafficking proposal first introduced in the 114th Congress: the Botnet Prevention Act of 2016.[281] That legislation faced criticism from those who feared it would criminalize valid cybersecurity research among other things.[282] Proponents

[268] United States v. Smith, 950 F.3d 893, 895 (D.C. Cir. 2020) (citing United States v. Gatling, 96 F.3d 1511, 1518 (D.C. Cir. 1996)). For a detailed examination of federal conspiracy law, *see, e.g.*, CRS Report R41223, *Federal Conspiracy Law: A Brief Overview*, by Charles Doyle.

[269] *See supra* note 263 and accompanying discussion.

[270] *Id.*

[271] 18 U.S.C. § 371.

[272] *See supra* § "Remedies and Penalties."

[273] Tex. Bus. & Com. Code Ann. § 324.055 (West).

[274] President Barack Obama, Remarks by the President at the National Cybersecurity Communications Integration Center (Jan. 13, 2015), *reprinted at* 2015 WL 163517, at *3 ("[W]e're proposing to update the authorities that law enforcement uses to go after cyber criminals. We want to be able to better prosecute those who are involved in cyber attacks, those who are involved in the sale of cyber weapons like botnets and spyware.").

[275] *See, e.g.*, Defending American Security from Kremlin Aggression Act of 2019, S. 482, 116th Cong. (2019).

[276] *Id.*

[277] The relevant provision is titled "Stopping Trafficking in Botnets; Forfeiture." *Id.* § 406.

[278] *Id.*

[279] *Id.*

[280] *Id.*

[281] S. 2931, 114th Cong. (2016).

[282] Letter from Access Now et al., to Senate (June 1, 2016), https://www.eff.org/document/coalition-letter-opposing-botnet-prevention-act.

have countered that proposals to prohibit botnet trafficking would be sufficiently limited by the legislation's intent requirements.[283]

Hacking Back

Another issue that has garnered legal,[284] academic,[285] media,[286] and legislative[287] attention is that of "hacking back"—where the victim of hacking launches an invasive counterattack against the initial hacker.[288] Hacking back has been the subject of significant policy debate.[289] Critics argue that hacking back could result in escalation and retaliation[290] and harm innocent parties though misattribution of the source of a cyber-attack.[291] Others have cautioned that hacking back could cause private actors to inadvertently wade into the realm of cyberwarfare and foreign relations if they hack back against an initial aggressor who turns out to be the agent of a foreign state.[292] Much of the recent scholarship on hacking back has been in this vein,[293] but hacking back has its

[283] *See* U.S. Dep't of Justice, *Prosecuting the Sale of Botnets*, *supra* note 255 (defending proposal to prohibit botnet trafficking on grounds that "proposal requires that the government . . . [meet] the burden to prove, beyond a reasonable doubt, that the individual intentionally undertook an act (trafficking in a means of access) that he or she knew to be wrongful").

[284] *See, e.g.*, U.S. DEP'T OF JUSTICE, BEST PRACTICES FOR VICTIM RESPONSE AND REPORTING OF CYBER INCIDENTS 23 (2018), https://www.justice.gov/criminal-ccips/file/1096971/download#page=23 (discussing hacking back).

[285] *See, e.g.*, Shane Huang, *Proposing A Self-Help Privilege for Victims of Cyber Attacks*, 82 GEO. WASH. L. REV. 1229, 1233 (2014).

[286] *See, e.g.*, Nicholas Schmidle, *Vigilantes Who Hack Back*, NEW YORKER (Apr. 30, 2018), https://www.newyorker.com/magazine/2018/05/07/the-digital-vigilantes-who-hack-back.

[287] *See, e.g.*, Active Cyber Defense Certainty Act, H.R. 3270, 116th Cong. (2019).

[288] *See* Beale, *supra* note 1, at 189 n.190 (describing hacking back). Related terms include, "counterstrikes, 'active defense,' 'back hacking,' 'retaliatory hacking,' or 'offensive countermeasures'" *Id.* at 190 (quoting Sean L. Harrington, *Cyber Security Active Defense: Playing with Fire or Sound Risk Management?* 20 RICH. J.L. & TECH. 12, 4 (2014)).

[289] *Compare* Josephine Wolff, *Attack of the Hack Back*, SLATE (Oct. 17, 2017), https://slate.com/technology/2017/10/hacking-back-the-worst-idea-in-cybersecurity-rises-again.html (proclaiming hacking back "[t]he worst idea in cybersecurity") *and* Martin Giles, *Five Reasons "Hacking Back" is a Recipe for Cybersecurity Chaos*, MIT TECH. REV. (June 21, 2019), https://www.technologyreview.com/2019/06/21/134840/cybersecurity-hackers-hacking-back-us-congress/ (describing hacking back as a "terrible idea"), *with* KERR, *supra* note 7, at 133 (summarizing debate over hacking back and collecting articles arguing in favor of hacking back) *and* Michael Edmund O'Neill, *Old Crimes in New Bottles: Sanctioning Cybercrime*, 9 GEO. MASON L. REV. 237, 277 (2000) ("In other words, just as settlers in the American West could not reliably count on the local sheriff to protect them, and instead kept a weapon handy to stymie potential aggressors, Internet users may need to protect themselves.").

[290] Josephine Wolff, *When Companies Get Hacked, Should They Be Allowed to Hack Back?*, ATLANTIC (July 14, 2017), https://www.theatlantic.com/business/archive/2017/07/hacking-back-active-defense/533679/ (summarizing concern of security advocates that hacking back "will merely serve as a vehicle for more attacks and greater chaos, particularly if victims incorrectly identify who is attacking them, or even invent or stage fake attacks from adversaries as an excuse for hacking back").

[291] *See, e.g.*, Beale, *supra* note 1, at 198 (summarizing view that due to difficulty in accurately attributing the source of a cyber-attack, that "remedial actions risk collateral damage to innocent parties").

[292] *See* PATRICK LIN, ETHICS OF HACKING BACK: SIX ARGUMENTS FROM ARMED CONFLICT TO ZOMBIES 15 (2016), http://ethics.calpoly.edu/hackingback.pdf ("Regardless of attribution, hacking back against a foreign target may be misinterpreted by the receiving nation as a military response from our state, to serious political and economic backlash.").

[293] *See, e.g.*, CTR. FOR CYBER & HOMELAND SEC., GEO. WASH. UNIV., INTO THE GRAY ZONE: THE PRIVATE SECTOR AND ACTIVE DEFENSE AGAINST CYBER THREATS 27 (2016), http://cchs.auburn.edu/_files/into-the-gray-zone.pdf ("First, 'hacking back' by the private sector to intentionally cause substantial harm and destroy other parties' data is clearly unauthorized and rightly prohibited."); *accord* Giles, *supra* note 289 (critiquing hacking back).

proponents who argue, among other things, that hacking back is necessary to "establish attribution of an attack, . . . retrieve and destroy stolen files, [and] monitor the behavior of an attacker."[294] In addition, it has been suggested that hacking back could be particularly useful in its "ability to prevent future [cyber] attacks by combatting existing botnets."[295]

The debate over hacking back is largely academic, as it appears that much hacking back is currently illegal—at least when conducted by private actors.[296] Although federal courts have not resolved the issue, the weight of persuasive authority suggests that the same provisions of the CFAA that prohibit hacking—such as § 1030(a)(5)'s prohibition against certain damage to computers—also generally prohibit hacking back by the victim of the initial attack.[297] At least one legislative proposal introduced in the 116th Congress would aim to authorize certain self-help measures. The Active Cyber Defense Certainty Act would create two new exceptions to the CFAA that would clarify that the law does not prohibit hacking back.[298] First, the Active Cyber Defense Certainty Act would amend the CFAA to expressly permit certain attributional technologies used to identify cyber intruders.[299] Second, with exceptions, the proposal would create an exclusion from CFAA prosecution for active cyber defense measures, which include defensive measures "consisting of accessing without authorization" the attacker's computer to gather information necessary to determine attribution, disrupt certain continued authorized activity, or monitor the behavior of an attacker to create "cyber defense techniques."[300] Such

---

[294] Press Release, Congressman Tom Graves, Graves, Gottheimer Introduce the Active Cyber Defense Certainty Act (June 13, 2019), https://tomgraves.house.gov/news/documentsingle.aspx?DocumentID=401122.

[295] Beale, *supra* note 1, at 191.

[296] *See, e.g.*, U.S. DEP'T OF JUSTICE, BEST PRACTICES FOR VICTIM RESPONSE, *supra* note 284, at 23 (cautioning that "[r]egardless of the victim's motive" it is possible that "accessing, modifying, or damaging a computer it does not own or operate" will "violate federal law and possibly also the laws of many states and foreign countries, if the accessed computer is located abroad.").

The CFAA has a carve out for certain law enforcement activity, which provides that: "This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States." 18 U.S.C. § 1030(f).

Although beyond the scope of this Report, it is worth observing that the federal wiretapping statute, 18 U.S.C. § 2511, contains the following carve out applicable to certain acts of hacking back conducted under color of law:

> (i) It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer, if--
>
> (I) the owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer;
>
> (II) the person acting under color of law is lawfully engaged in an investigation;
>
> (III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and
>
> (IV) such interception does not acquire communications other than those transmitted to or from the computer trespasser.

18 U.S.C. § 2511(2)(i).

[297] *E.g.*, U.S. DEP'T OF JUSTICE, BEST PRACTICES FOR VICTIM RESPONSE, *supra* note 284, at 23; Orin Kerr, *The Legal Case Against Hack-Back: A Response to Stewart Baker*, STEPTOE CYBERBLOG (Nov. 2, 2012), https://www.steptoecyberblog.com/2012/11/02/the-hackback-debate/; Beale, *supra* note 1, at 191; CTR. FOR CYBER & HOMELAND SEC., GEO. WASH. UNIV., *supra* note 293; *but see* Stewart Baker, *RATs and Poison Part II: The Legal Case for Counterhacking*, STEPTOE CYBERBLOG (Nov. 2, 2012), https://www.steptoecyberblog.com/2012/11/02/the-hackback-debate/ (arguing that hacking back may not be a violation of the CFAA).

[298] Active Cyber Defense Certainty Act, H.R. 3270, 116th Cong. (2019).

[299] *Id.*

[300] *Id.*

cyber defense measures would generally require notification to, and pre-approval by, the FBI.[301] The Active Cyber Defense Certainty Act was previously introduced in the 115th Congress.[302]

Author Information

Peter G. Berris
Legislative Attorney

Disclaimer

[301] *Id.*

[302] Active Cyber Defense Certainty Act, H.R. 4036, 115th Cong. (2017).